



Лаптев О.А., Савченко В.А., Шуклін Г.В.

**Виявлення та блокування засобів негласного
отримання інформації на об'єктах інформаційної
діяльності**

Навчальний посібник

Київ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО
ЗАХИСТУ

**Виявлення та блокування засобів негласного отримання інформації на
об'єктах інформаційної діяльності**

Навчальний посібник по дисципліні *Методи та засоби технічного захисту
інформації*

Для студентів ННІЗІ

Затвержено до друку вченою радою Навчально-наукового інституту захисту
інформації (протокол № 3 від 16.09.2020 р.).

Київ -2020

ЗМІСТ

| | |
|---|----|
| Вступ..... | 4 |
| 1. Загальні положення..... | 5 |
| 2. Класифікація закладних пристроїв і їх демаскуючих ознак..... | 7 |
| 3. Технічні засоби пошуку ЗП та інших засобів негласного знімання інформації | 9 |
| 4. Зміст і послідовність робіт з підготовки і проведення комплексних спеціальних перевірок приміщень | 11 |
| 5. Методика виконання робіт на підготовчому етапі | 15 |
| 6. Методика виконання робіт на етапі безпосереднього проведення комплексної перевірки | 18 |
| 6.1. Пошук закладних пристроїв з радіочастотним каналом передачі... | 20 |
| 6.1.1. Сканування радіочастотного діапазону, аналіз радіоелектронної обстановки в приміщенні, виявлення радіовипромінювальних ЗП за допомогою ПАК DigiScan..... | 20 |
| 6.1.2. Локалізація місця розташування радіовипромінювальних ЗП за допомогою пошукового приладу ST 031 «Піранья»..... | 26 |
| 6.1.3. Пошук і виявлення активних радіовипромінювальних ЗП за допомогою детектора поля PROTECT 2103 | 32 |
| 6.2. Пошук закладних пристроїв, що використовують провідні комунікації | 35 |
| 6.3. Пошук закладних пристроїв, що використовують низькочастотні магнітні випромінювання | 37 |
| 6.4. Пошук закладних пристроїв, що використовують інфрачервоне випромінювання | 39 |
| 6.5. Пошук пасивних закладних пристроїв | 40 |
| 6.6. Дослідження приміщень на предмет наявності акустичного і віброакустичного каналів витоку інформації | 44 |
| 6.7. Візуальний огляд і фізичний пошук закладних пристроїв | 48 |
| 7. Методика виконання робіт на заключному етапі комплексної перевірки приміщень | 52 |
| Висновок | 54 |
| Список використаної літератури | 55 |

ДОДАТКИ

Додаток 1. Варіант плану проведення комплексної спеціальної перевірки приміщень.

Додаток 2. Методика пошуку закладних пристроїв з використанням пошукового програмно-апаратного комплексу ПАК DigiScan .

Додаток 3. Методика пошуку закладних пристроїв з використанням пошукового приладу ST 031 «Піранья».

Додаток 4. Методика пошуку закладних пристроїв з використанням нелінійного локатора NR -900 EM .

Додаток 5. Методика пошуку закладних пристроїв з використанням індикатора поля PROTECT 1203.

Додаток 6. Варіант акту комплексної спеціальної перевірки приміщень.

Додаток 7. Варіант рекомендацій щодо підвищення захищеності перевірених приміщень і об'єктів.

Додаток 8. Перелік нормативно-правових документів, на основі яких здійснюється діяльність з надання послуг з ТЗІ.

ВСТУП

В умовах конкурентної боротьби на міжнародному ринку масштаби промислової розвідки різко зростають. Все ширше використовуються плоди науково-технічного прогресу. Промислова розвідка стає більш гнучким і витонченим засобом отримання інформації.

Держава своїми законами і підзаконними актами визначила саме поняття комерційної таємниці, право підприємців на її захист від розголошення і розкрадання інформації. Визначена адміністративна і кримінальна відповідальність громадян України за порушення прав власності власника закритої комерційної інформації. Однак, безпечність людей і поки ще недосконалість законодавства дозволяють зловмисникам безкарно вилучати у власників їх цінну комерційну інформацію, що приносить величезні матеріальні та моральні втрати. Розкрадання інформації проводиться за допомогою застосування технічних засобів негласного знімання інформації, так званих закладних пристроїв.

Закладні пристрої (ЗП) – це спеціальні технічні засоби, які таємно встановлюються в приміщеннях, автомобілях, офісному обладнанні та інших об'єктах шпигунства, і призначені для негласного знімання інформації (НЗІ) акустичного або видового характеру.

Різноманіття напрямків і методів прослуховування зумовило розвиток різних організаційних і технічних способів захисту. Найбільш важливим і ефективним методом технічного захисту інформації є виконання комплексних спеціальних перевірок приміщень та інших об'єктів з пошуком і нейтралізацією засобів НЗІ.

Мета проведення комплексних спеціальних перевірок – пошук закладних пристроїв, дослідження рівня захищеності приміщень і видача рекомендацій щодо підвищення його інформаційної безпеки.

Методика виявлення джерел акустичної або відеоінформації регламентує сутність, перелік і послідовність виконуваних робіт інструментального та фізичного пошуку закладних пристроїв, дослідження рівня захищеності об'єктів, що перевіряються, а також звітну та облікову документацію, яка оформляється за результатами перевірки.

В даній Методиці використовуються рекомендації та термінологія, наведені в «Положенні про технічний захист інформації в Україні», Державному стандарті України ДСТУ 3396.2-97, «Інструкції відносно умов і правил Здійснення діяльності у Галузі технічного захисту інформації та контролю за їх Дотриманням».

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Одним з головних способів комплексного захисту інформації є проведення комплексу організаційних і технічних заходів з обстеження приміщень з метою виявлення технічних каналів витоку інформації; знешкодження виявлених закладних пристроїв; розробка рекомендацій та проведення заходів щодо закриття виявлених каналів витоку інформації; підбір, установка, монтаж, налагодження технічних засобів захисту інформації та технічних засобів контролю ефективності заходів захисту інформації

В основі виконання робіт з технічного захисту інформації лежать наступні принципи:

- правозаконності (відповідність діяльності підприємства законам і нормативним актам України);
- конфіденційності при виконанні робіт;
- відповідальності перед клієнтами та партнерами, точне виконання всіх зобов'язань;
- забезпечення високої якості послуг, першокласних характеристик і споживчих властивостей продукції і послуг, що надаються при мінімальній їх вартості;
- найсуворіший контроль надійності і якості продукції і виконуваних послуг на всіх етапах роботи: від розробки ідеї і вибору комплектуючих і технічних засобів до оформлення результатів роботи;
- швидка реакція на запити ринку, надання послуг на основі кращих вітчизняних і зарубіжних технологій і технічних рішень.

Для якісного виконання вирішуваних завдань, потрібно мати у своєму розпорядженні найсучаснішу спеціальну пошукову техніку, методичну та нормативну літературу, висококласних фахівців.

До теперішнього часу накопичено чималий досвід організації і проведення пошукових робіт по виявленню впроваджених в приміщеннях, предметів, електронних приладів та інших засобів обробки інформації для несанкціанованого отримання інформації.

Аналіз накопиченого вітчизняного і світового досвіду в сфері інформаційної безпеки дозволяє зробити висновок, що найбільш повними за обсягом і нумерацією проведених робіт є **комплексні спеціальні перевірки приміщень**, методика проведення яких представлена в цьому підручнику.

Мета проведення комплексних спеціальних перевірок полягає в припиненні (запобіганні) витоку інформації, що захищається з обстежуваних приміщень за допомогою засобів НЗІ, що дозволить запобігти збитку, який

може бути нанесений власнику, користувачеві, що захищається в разі несанкціонованого використання цієї інформації.

Основні завдання комплексних спеціальних перевірок:

- виявлення і нейтралізація впроваджених засобів НЗІ;
- виявлення незакритих потенційних технічних каналів витоку інформації (ТКВІ) (тобто тих, які при наявності певних умов можуть бути використані для несанкціонованого знімання інформації);
- визначення заходів, необхідних для закриття (ліквідації) виявлених потенційних ТКВІ;
- збір відомостей про тактику застосування засобів НЗІ і їх характеристики.
- роботи з пошуку і знешкодження ЗП виконуються фізичними особами, організаціями та підприємствами, які мають спеціальний дозвіл (ліцензію) на право здійснення діяльності в галузі технічного захисту інформації (ТЗІ) відповідно до планів, технічних завдань, договорів, директивних вказівок і т. д.

Обстеженню підлягають:

- елементи конструкції приміщень;
- технічні засоби забезпечення інформаційної діяльності (далі - технічні засоби);
- предмети інтер'єру та інші предмети.

Основні принципи організації та проведення комплексних спеціальних перевірок:

- правозаконності - відповідність положенням законів та інших правових актів, що регулюють відносини у сфері захисту інформації;
- конфіденційність підготовки і виконання робіт;
- системність (періодичність) проведення перевірок;
- взаємозв'язок з іншими заходами в загальній системі захисту інформації;
- комплексність застосовуваних методів і технічних засобів;
- достатність проведених робіт для достовірної оцінки захищеності приміщень;
- комплексність розроблюваних організаційних, інженерних і технічних заходів захисту;
- достатність рекомендованих заходів захисту для запобігання витоку інформації за виявленими потенційним ТКВІ.

Методологія і порядок пошуку ЗП встановлюється з урахуванням їх класифікації, характеристик об'єкта, який підлягає перевірці, складу використовуваних пошукових технічних засобів.

2. КЛАСИФІКАЦІЯ ЗАКЛАДНИХ ПРИСТРОЇВ ТА ЇХ ДЕМАСКУЮЧІ ОЗНАКИ

Закладні пристрої (ЗП) - це таємно встановлені технічні пристрої, призначені для негласного знімання наступних видів інформації:

- акустичної (мовної) інформації в приміщеннях;
- відеоінформації в приміщеннях;
- телефонних переговорів;
- інформації, що обробляється в спеціальних технічних засобах: ПК, факси, ксерокси та ін.

Закладні пристрої можна класифікувати за кількома ознаками:

1. За методом знімання інформації:

- ЗП знімання мовної інформації з використанням акустoeлектричних перетворювачів;
- ЗП знімання мовної та іншої інформації, яка циркулює в електричних ланцюгах технічних засобів;
- ЗП знімання інформації видового характеру з використанням систем прихованого відеоспостереження.

2. За частотним діапазоном каналу передачі:

- мікрофони та інші акустoeлектричні перетворювачі мовного діапазону частот;
- надтональні мікропередавачі (0,1 - 1 МГц);
- радіомікрофони і радіопередавачі (0,02 - 1,5 ГГц);
- передавачі інфрачервоного (ІЧ) діапазону хвиль (750 - 1150 нм);

Наведені діапазони частот відповідають основним типам ЗП.

3. За видом електроживлення:

- ЗП, які не вимагають джерела електроживлення (динамічні мікрофони та інші акустoeлектричні перетворювачі, що мають мікрофонний ефект);
- ЗП з живленням від автономного джерела (акумулятор, хімічний елемент та ін.);
- ЗП з живленням від електромережі або лінії зв'язку, котрі знаходяться під напругою.

4. За режимом роботи в контрольований момент часу:

- активні - знаходяться в увімкненому стані;
- пасивні - знаходяться в вимкненому стані.

5. За типом активізації (включення) в роботу:

- постійно включені;
- з акустопуском - включаються після перевищення рівня акустичного шуму над заданим значенням;
- з дистанційним включенням;

- з програмно-тимчасовим включенням.

б. За використовуваним каналом передачі інформації:

- ЗП, що використовують радіочастотний канал передачі;

- ЗП, що використовують провідні канали передачі;

- ЗП, що використовують канали передачі на основі низькочастотних електромагнітних полів;

- ЗП, що використовують інфрачервоні канали передачі.

Широкий спектр принципів дії, використовуваних методів і технологій знімання і передачі інформації зумовив значну кількість різнорідних ознак, за якими можна виявити закладний пристрій.

Сутність пошуку ЗП полягає в виявленні, локалізації та розпізнаванні демаскуючих ознак, які притаманні практично всім закладним пристроям:

1) випромінвані електромагнітні поля радіочастотного каналу передачі;

2) інформаційні сигнали в провідних комунікаціях;

3) електромагнітні випромінювання низької частоти з переважанням магнітної складової;

4) інфрачервоне випромінювання, модульоване мовним сигналом;

5) наявність напівпровідникових приладів у пасивних ЗП, що дають відгук на зондуючий високочастотний сигнал;

б) демаскуючі ознаки, що визначаються візуальним шляхом.

Відповідно до демаскуючих ознак визначаються:

- склад спеціальних пошукових засобів і інструментів для виявлення демаскуючих ознак з найбільшою достовірністю;

- послідовність і перелік робіт з пошуку ЗП на кожному етапі проведення комплексної спеціальної перевірки приміщень;

- особливості інструментального пошуку ЗП при застосуванні кожного виду пошукового обладнання;

- особливості фізичного (візуального) пошуку ЗП із застосуванням комплексу пошукових дзеркал і інших інструментів;

- особливості ідентифікації та локалізації місця розташування ЗП.

В процесі виконання перевірок приміщень проводиться також обстеження їх на предмет наявності можливих технічних каналів витоку інформації (ТКВІ). Зокрема такими каналами є акустична проникність будівельних конструкцій, віброакустична провідність комунікаційних систем, трубопроводів водопроводу та опалення, системи вентиляції та інші. На рис. 1 подано класифікацію обстежуваних каналів витоку інформації, пошукове обладнання і очікувані результати інструментального контролю.

3. ТЕХНІЧНІ ЗАСОБИ ПОШУКУ ЗП ТА ІНШИХ ЗАСОБІВ НЕГЛАСНОГО ЗНІМАННЯ ІНФОРМАЦІЇ

Для виконання інструментального контролю при проведенні пошукових заходів і дослідженні приміщень на наявність можливих каналів витоку інформації під час виконання спеціальної комплексної перевірки використовується спеціальне пошукове обладнання. Перелік використовуваного обладнання та його призначення представлені в таблиці 1.

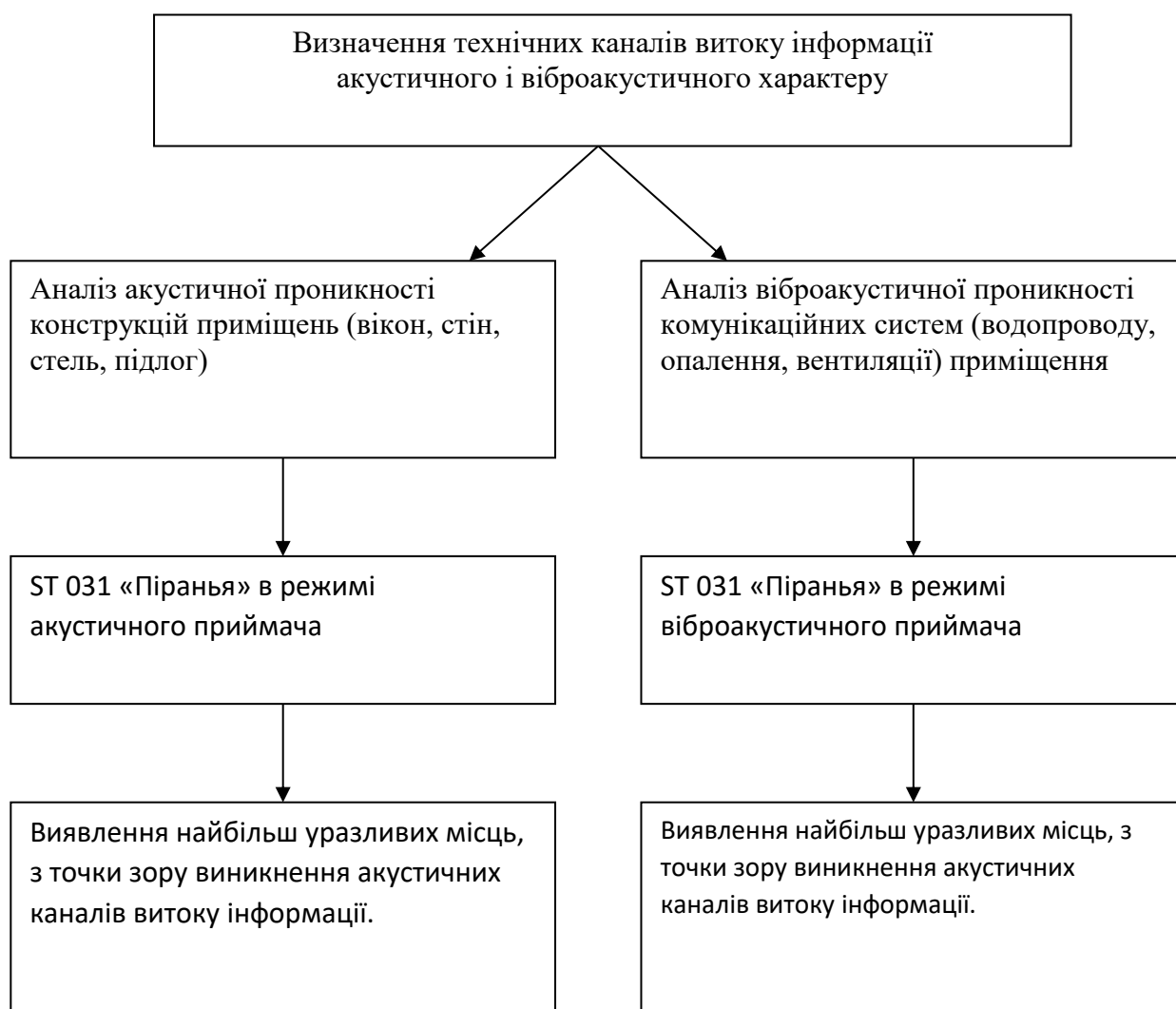


Рис. 1. Виявлення акустичних і віброакустичних ТКВІ і тип пошукового обладнання

Перелік спеціального пошукового обладнання

Таблиця 1

| № | Найменування устаткування | Призначення обладнання |
|----|---|--|
| 1 | 2 | 3 |
| 1. | Пошуковий програмно-апаратний комплекс DigiScan (або аналогічний) в складі: - портативний комп'ютер; - спеціальне програмне забезпечення DigiScan -2000; - скануючий приймач AR - 3000 А . | Аналіз радіоелектронної обстановки на об'єкті, що перевіряється в широкому діапазоні частот 0,1 - 2036 МГц, пошук радіовипромінювальних ЗП з будь-яким видом модуляції, а також ЗП, що використовують як відкритий радіоканал, так і радіоканал з інверсією спектру. |
| 2. | Багатофункціональний пошуковий прилад ST 031 «Піранья». | Виявлення та локалізація: - радіовипромінювальних ЗП, - ЗП, які працюють з випромінюванням в ПЧ-діапазоні; - ЗП, що використовують для передачі провідні лінії різних комунікацій; - джерел ЕМП з переважанням магнітної складової поля; - трас прокладки прихованої електропроводки; - можливих акустичних і віброакустичних каналів витoku інформації. |
| 3. | Нелінійний локатор NR 900 EM . | Пошук ЗП, що містять напівпровідникові компоненти, незалежно від їх функціонального стану, в тому числі пасивних ЗП, засобів звукозапису, ЗП вмонтованих в елементи інтер'єру і будівельних конструкціях - підлогах, стелях, стінах. |
| 4. | Портативний частотомір RFM -32. | Автозахоплення частоти електромагнітного поля з найбільшим рівнем сигналу і аналіз частот діючих радіопередавачів в широкому діапазоні частот 10 --3000 МГц. |
| 5. | Індикатор поля PROTECT 1203 | Оперативний пошук і локалізація всіх видів випромінюючих ЗП, в тому числі і цифрових передавачів, а також передавачів з інверсією спектру. |

Вибір даних технічних пристроїв і їх характеристик був обґрунтований з урахуванням досягнення наступних цілей:

- максимально можлива достовірність отриманих результатів;
- можливість комплексування різних методів пошуку;
- максимальна повнота інструментального контролю - можливість виявлення всіх демаскуючих ознак і всіх видів ЗП та інших засобів НДІ;
- зниження рівнів ймовірності пропуску та ймовірності "помилкової тривоги";

- використання передових методів і технологій інструментального контролю, що дозволяють проводити пошук з максимальною ефективністю;
- достатність комплексу обладнання для інструментального пошуку всіх сучасних ЗП.

4. ЗМІСТ І ПОСЛІДОВНІСТЬ РОБІТ З ПІДГОТОВКИ ТА ПРОВЕДЕННЯ КОМПЛЕКСНИХ СПЕЦІАЛЬНИХ ПЕРЕВІРОК ПРИМІЩЕНЬ

Метою проведення спеціальної комплексної перевірки приміщень є:

1. припинення (запобігання) витоку інформації, що захищається з обстежуваних приміщень;
2. пошук (виявлення, локалізація і ідентифікація) таємно встановлених ЗП та інших засобів НДІ;
3. дослідження приміщень для виявлення можливих ТКВІ;
4. розробка і видача замовнику рекомендацій щодо усунення ТКВІ і підвищенню захищеності приміщень, що перевіряються;
5. подання замовнику підсумкових і звітних документів по виконаних роботах.

Спеціальна комплексна перевірка організується керівником підприємства (Виконавцем), що надає послуги з технічного захисту інформації і пошуку закладних пристроїв, на підставі Договору з Замовником. Комплекс заходів з перевірки виконується фахівцями підприємства Виконавця, що має на даний вид діяльності відповідну державну ліцензію Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

Всі заходи з проведення комплексної спеціальної перевірки умовно діляться на три етапи:

1. Підготовчий етап.
2. Етап безпосереднього проведення перевірки.
3. Заключний етап.

Роботи, що становлять зміст *підготовчого етапу* представлені в таблиці 2.

Зміст підготовчого етапу перевірки

Таблиця 2

| № п/п | Зміст робіт |
|----------|---|
| 1 | 2 |
| 1. | Уточнення переліку інформації, що захищається і ступеня її важливості |
| 2. | Аналіз передумов підозр, визначення ймовірного суб'єкта, який здійснює перехоплення інформації, оцінка його можливостей і тактики дій |
| 3. | Попередній огляд приміщень і контрольованої території |
| 4. | Попередній збір даних і аналіз радіоелектронної обстановки в районі проведення пошукових робіт |
| 5. | Вивчення планів приміщень, схем комунікацій, зв'язку, організації охорони і т.п. |
| 6. | <p>Розробка плану проведення комплексної спеціальної перевірки приміщень:</p> <ul style="list-style-type: none"> - узгодження цільової установки: для протидії якого суб'єкта слід провести пошукові заходи; - узгодження масштабу і місця проведення пошукових заходів; - узгодження часу проведення перевірки; - узгодження варіанту прикриття, під яким буде проводитися перевірка(відпрацювання заходів щодо збереження конфіденційності проведеної перевірки); - узгодження заходів щодо активізації впроваджених засобів НДІ; - узгодження варіантів дій при виявленні засобів НДІ. |
| 7. | Розробка переліку робіт, переліку необхідної апаратури та інструментів |
| 8. | Розподіл залучених сил і засобів по об'єктах і видах робіт |
| 9. | Уточнення приватних методик використання залученої апаратури в конкретних умовах майбутньої перевірки |
| 10. | Оформлення плану проведення комплексної спеціальної перевірки приміщень та затвердження його Замовником |
| 11. | Підготовка бланків, схем, заготовок інших документів, необхідних для проведення всього комплексу робіт |
| 12. | Підготовка апаратури для проведення пошукових і дослідницьких робіт |

Частина робіт цього етапу передбачає участь в них керівника підприємства, на якому повинна бути проведена перевірка. Заходи за погодженням деяких етапів перевірки доцільно проводити поза стінами приміщення, яке перевіряється для збереження конфіденційності майбутньої перевірки.

Варіант плану проведення комплексної спеціальної перевірки приміщень представлений в додатку 1.

Етап безпосереднього проведення комплексної спеціальної перевірки приміщень.

Зміст другого етапу робіт з проведення комплексної спеціальної перевірки приміщень включає безпосереднє проведення в приміщеннях запланованих пошукових заходів. Перед початком безпосереднього проведення пошукових робіт проводиться огляд прилеглих до досліджуваного приміщення вулиць і територій. При цьому особлива увага звертається на осіб, що користуються навушниками, автомобілі з людьми, які тривалий час перебувають на одному місці, автомобілі з зовнішньою антеною, вставленим в прикурювач адаптером, тонованими або завішеними вікнами. У приміщенні, яке перевіряється, по можливості, закриваються двері, вікна, штори, жалюзі для виключення візуального контакту з можливим спостерігачем з боку вулиці або сусідніх приміщень. Для маскуванню шумів, створюваних пошуковою апаратурою, включається наявна звуковідтворююча апаратура (радіо, магнітола і т.п.). Зміст і послідовність робіт, які проводяться на цьому етапі, представлені в таблиці 3.

Зміст етапу безпосереднього виконання перевірки

Таблиця 3

| № п/п | Зміст робіт | Застосоване пошукове обладнання |
|-------|--|---|
| 1 | 2 | 3 |
| 1. | Візуальний огляд огорожувальних конструкцій, предметів інтер'єру | RFM -32; набір дзеркал. |
| 2. | Виконання запланованих заходів щодо активізації впроваджених ЗП та інших засобів НДІ | |
| 3. | Сканування радіочастотного діапазону, аналіз радіоелектронної обстановки в приміщенні, виявлення радіовипромінювальних ЗП | ПАК DigiScan; ST 031 «Піранья»; PROTECT 1203; RFM -32. |
| 4. | Перевірка ліній та обладнання провідних комунікацій: - силової та освітлювальної електромережі; - офісної та абонентської телефонної мережі; - пожежної та охоронної сигналізації; - інших провідних комунікацій, в тому числі нез'ясованого призначення | ST 031 «Піранья» |
| 5. | Виявлення джерел низькочастотних магнітних полів, трас прокладки прихованої (непозначеної) електропроводки | ST 031 «Піранья» |

| 1 | 2 | 3 |
|----|--|----------------------------|
| 6. | Перевірка випромінювань в інфрачервоному діапазоні хвиль | |
| 7. | Перевірка елементів будівельних конструкцій, предметів інтер'єру з використанням нелінійного локатора для пошуку пасивних ЗП | NR 900 ME |
| 8. | Дослідження звукопроникності елементів конструкцій, перевірка інженерно-технічних комунікацій на наявність в них акустичних та віброакустичних сигналів із приміщень | ST 031 «Піранья» |
| 9. | Фізичний пошук ЗП за результатами інструментального контролю, а також пошук ЗП, що мають візуальні демаскуючі ознаки | RFM -32; набір дзеркал. |

Приватні методики проведення пошукових робіт з використанням конкретного обладнання представлені в додатках 2-5.

Заключний етап комплексної спеціальної перевірки приміщень.

На заключному етапі роботи виконуються в основному за межами підприємства, що перевіряється, в приміщеннях організації, яка проводить перевірку. Зміст заключного етапу представлено в таблиці 4. Крім того, в додатку 6 представлений варіант акту комплексної спеціальної перевірки приміщень. У додатку 7 представлений варіант рекомендацій щодо підвищення захищеності приміщень і об'єктів.

Зміст заключного етапу перевірки

Таблиця 4

| № п/п | Зміст робіт |
|-------|---|
| 1 | 2 |
| 1. | Обробка результатів перевірки, оформлення протоколів вимірювань, проведення необхідних інженерних розрахунків. |
| 2. | Визначення технічних характеристик, споживчих властивостей виявлених ЗП, орієнтовного часу і способу їх впровадження. |
| 3. | Складання опису проведених робіт і досліджень з доданням необхідних схем і планів приміщень. |
| 4. | Розробка рекомендацій щодо підвищення захищеності приміщень, що перевіряються: <ul style="list-style-type: none"> - складання переліку і схем виявлених технічних каналів витоку інформації по кожному приміщенню; - оцінка ступеня існуючого захисту кожного приміщення від негласного знімання інформації по виявлених каналах її витоку; - розробка додаткових заходів і способів захисту по кожному каналу і приміщенню (організаційних, інженерних, технічних); |

| 1 | 2 |
|----|--|
| | <ul style="list-style-type: none"> - складання переліку технічних засобів і систем, рекомендованих до установки для захисту інформації від витоку технічними каналами; - розробка пропозицій по способах використання рекомендованих технічних засобів і систем і об'єднання їх в єдину, компактну систему захисту інформації. |
| 5. | Складання акту комплексної спеціальної перевірки приміщення. |
| 6. | Подання підсумкових і звітних документів керівнику підприємства для затвердження. |

5. МЕТОДИКА ВИКОНАННЯ РОБІТ НА ПІДГОТОВЧОМУ ЕТАПІ

Суть попереднього етапу полягає в зборі вихідних даних про об'єкт, попередньому огляді об'єкта, плануванню та узгодженню заходів, виконуваних під час перевірки.

Метою підготовчого етапу є розробка плану перевірки, затвердження його у Замовника, а також підготовка пошукового обладнання та облікової документації.

Перелік робіт, які виконуються на підготовчому етапі, надано в розділі 4 цієї Методики.

Частина заходів даного етапу, не пов'язаних з оглядом об'єкта, рекомендується проводити на нейтральній території для виключення підозр з боку можливих спостерігачів. Всі заплановані і виконувані заходи слід проводити без афішування, не привертаючи уваги співробітників, не втаємничених у питання перевірки.

Спочатку підготовчого етапу уточнюється перелік інформації, що захищається, ступінь її важливості, фізичні носії інформації, що захищається, можливі канали витоку. З'ясуванню також підлягають особливості та порядок доступу до інформації, що захищається на підприємстві Замовника, вживані заходи технічного захисту інформації, склад технічних засобів обробки інформації. Спільно з Замовником аналізуються передумови підозр по витоку інформації, уточнюється: чи є причиною можливих збитків можливий витік конфіденційної інформації технічними каналами, визначається ймовірний суб'єкт, який здійснює перехоплення інформації, оцінюються його можливості і тактика дій. Уточнюється використовувана апаратура для ТЗІ, режими і порядок її використання.

Для виконання якісного планування здійснюється попередній огляд приміщень і прилеглої території. При огляді контрольованої території з'ясовуються наступні дані:

- наявність території, що охороняється, її площа, огорожа, порядок охорони (патрулювання) території, наявність автостоянок, можливість ведення спостереження або знімання інформації з автомобілів, припаркованих поблизу території; наявність суміжних будівель, їх призначення і

віддалення від об'єкта, що перевіряється, оцінюється можливість ведення спостереження або знімання інформації з цих будівель;

- досліджується і попередньо аналізується радіоелектронна обстановка поблизу об'єкта, що перевіряється: за допомогою портативного частотомера RFM -32 заміряються і документуються частоти і рівні найбільш потужних радіосигналів по периметру контрольованої території. Дані вимірів: місце, частота, рівень сигналів відзначаються на схемі для подальшого аналізу і порівняння з радіоелектронною обстановкою всередині приміщення, яке перевіряється. Для більш детального вивчення радіоелектронної обстановки в районі об'єкта використовується сканування діапазону частот за допомогою програмно-апаратного комплексу ПАК DigiScan . При цьому всі дані по частотах і сигналах заносяться в електронну базу, що істотно знижує трудомісткість робіт під час перевірки.

При попередньому огляді приміщення з'ясовуються наступні дані:

- площа приміщення, тип і структура будівельних конструкцій (стіни, стелі, підлоги, перекриття, вікна);
- попереднє визначення можливих технічних каналів витоку інформації;
- з'ясовуються найбільш ймовірні місця таємної установки ЗП та інших засобів НДІ;
- наявність і стан меблів в приміщенні, яке перевіряється, наявність офісної техніки, порядок її використання;
- регулярність проведення прибирань, а також протирання пилу у важкодоступних місцях.

Спільно з Замовником:

- уточнюються результати попередніх перевірок з пошуку ЗП;
- з'ясовується час проведення останнього ремонту приміщення, хто проводив, приблизні обсяги ремонтних робіт, хто із співробітників курував і контролював виконання ремонтних робіт; оцінюється можливість вбудовування в будівельні конструкції закладних пристроїв;
- з'ясовуються у Замовника, які предмети інтер'єру і аксесуари були встановлені в приміщенні за останні три місяці (картини, квіткові горщики, меблі та ін.), А також їх походження.

При необхідності уточнення вихідних даних, отриманих в ході попереднього огляду, проводиться вивчення планів приміщень, схем комунікацій, зв'язку, організації охорони і т.п. При цьому уточнюються суміжні приміщення, досліджуються суміжні приміщення: яке підприємство, профіль господарської діяльності, суміжні комунікаційні системи (опалення, вентиляція та ін.). Особлива увага приділяється вивченню системи зв'язку, магістралі прокладки телефонних ліній, можливість несанкціонованого доступу до них ймовірного зловмисника, уточнюється тип офісної міні - АТС, хто відповідає за її програмування і інші питання для попереднього визначення можливих ТКВІ.

Разом з тим, у Замовника з'ясовуються випадки зовнішньої розвідки по відношенню до об'єкта, підозрілі відвідувачі, зовнішні спостерігачі та інші

передумови підозр, оцінюються можливі загрози фізичної або електронної безпеки.

Після цього здійснюється попереднє узгодження з Замовником для розробки плану перевірки:

- погоджується цільова установка: для протидії якому об'єкту слід проводити пошукові заходи;
- узгодження масштабу і місця проведення пошукових заходів;
- узгодження часу проведення перевірки;
- узгодження варіанту прикриття (легенди), під яким буде проводитися перевірка;
- узгодження заходів з відпрацювання конфіденційності проведеної перевірки;
- узгодження заходів щодо активізації впроваджених ЗП і засобів НДІ;
- узгодження варіантів дій в разі виявлення ЗП.

Як заходи щодо активізації впроваджених ЗП і засобів НДІ можна запланувати наступні:

- оголошення співробітникам підприємства про важливу нараду, намічену на запланований час перевірки;
- планування на день перевірки важливих переговорів, які потім несподівано будуть перенесені в інше приміщення або на інший час;
- створення або імітація акустичного фону робочої обстановки під час перевірки з використанням аудіомагнітофонів для відтворення раніше записаної мови.

Після уточнення вихідних даних і погоджень розробляється перелік робіт по перевірці приміщень, виходячи з якого визначається склад пошукового обладнання та інструментів для виконання кожного виду робіт. Уточнюється додаткове обладнання для виконання заходів щодо активізації впроваджених ЗП. Особливу увагу при плануванні слід приділити обсягом того чи іншого виду робіт. Заздалегідь визначається повнота і глибина пошукових заходів, а також можливість виконання контрольних операцій на основі альтернативних методів пошуку з метою зниження ймовірності пропуску закладних пристроїв.

На основі аналізу моделі безпеки досліджуваного об'єкта і з урахуванням наявних ресурсів уточнюється послідовність запланованих робіт і здійснюється розподіл сил і засобів по об'єктах і видах робіт. При цьому, першими перевіряються найбільш ймовірні і незакриті технічні канали витоку інформації.

Виходячи з отриманих даних в ході попереднього огляду, уточнюються приватні методики використання пошукового обладнання в конкретних умовах майбутньої перевірки.

На основі результатів попередніх досліджень і узгодження вищевказаних питань оформляється план проведення комплексної спеціальної перевірки приміщень (дод. 1).

Разом з планом готується облікова документація - бланки, схеми, заготовки інших документів, необхідні для проведення всього комплексу робіт.

На підготовчому етапі також виконується підготовка обладнання для проведення пошукових і дослідницьких робіт, яка включає в себе:

- перевірку комплектності;
- перевірку рівня заряду акумуляторів;
- перевірку працездатності обладнання в кожному із запланованих режимів роботи;
- стан чохла, тари, упаковки для прихованого перевезення на об'єкт, що перевіряється.

Таким чином, підготовчий етап має важливе значення в проведенні спеціальної комплексної перевірки, а якісне і повне виконання всіх заходів дозволить істотно підвищити достовірність результатів пошуку, знизити трудовитрати і тривалість виконання робіт на етапі безпосереднього проведення комплексної перевірки.

6. МЕТОДИКА ВИКОНАННЯ РОБІТ НА ЕТАПІ БЕЗПОСЕРЕДНЬОГО ПРОВЕДЕННЯ КОМПЛЕКСНОЇ ПЕРЕВІРКИ

Методологія і порядок інструментального пошуку ЗП визначається класифікацією демаскуючих ознак, а також типами і характеристиками пошукових технічних засобів, які використовуються і повинні забезпечити високу ефективність виявлення, локалізації та ідентифікації ЗП.

Весь процес пошуку ЗП логічно об'єднує інструментальний пошук і фізичний пошук (рис.3). Інструментальний пошук активних ЗП (п. 6.1 - 6.4) здійснюється за їх демаскуючими ознаками, до яких відносяться:

- електромагнітні поля радіочастотного каналу передачі;
- сигнали акустично-електричного перетворення в провідних комунікаціях;
- електромагнітні випромінювання низької частоти з переважанням магнітної складової;
- інфрачервоне випромінювання, модульоване мовними сигналами.

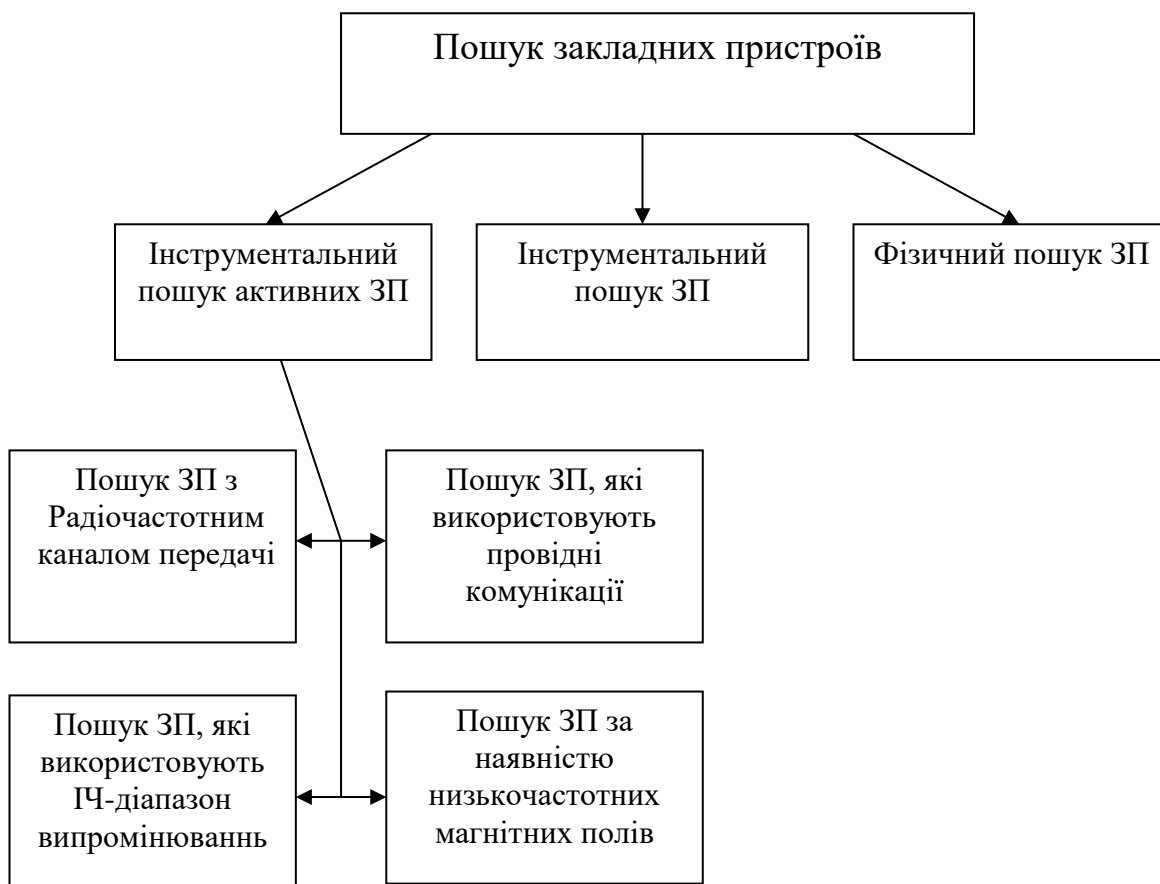


Рис.3. Взаємозв'язок пошукових заходів відповідно до класифікації демаскуючих ознак закладних пристроїв

Інструментальний пошук пасивних ЗП здійснюється методом нелінійної локації на основі аналізу гармонік відображень зонduючого НВЧ сигналу (п. 6.5).

Візуальний огляд і фізичний пошук ЗП є основним видом пошуку і проводиться на основі результатів інструментального пошуку і з урахуванням виявлених демаскуючих ознак (п.6.6).

Крім зазначених робіт з пошуку ЗП, проводиться дослідження звукопроникності елементів будівельних конструкцій, перевірка звукопровідності інженерно-технічних комунікацій на наявність в них акустичних та віброакустичних каналів витоку інформації з приміщень, що перевіряються (п. 6.7).

6.1. Пошук закладних пристроїв з радіочастотним каналом передачі інформації.

Пошук ЗП та інших засобів НДІ з радіочастотним каналом передачі здійснюється на основі радіомоніторингу. Під радіомоніторингом розуміється детальне дослідження радіообстановки на об'єкті, що перевіряється, постійне спостереження за радіосигналами і їх частотами.

Основною метою радіомоніторингу при обстеженні об'єктів підприємницької діяльності є виявлення радіосигналу, визначення його частоти, смуги пропускання, дослідження сигналу по кореляційних функціях, амплітудних і спектральних характеристиках, виявлення наявності гармонік, класифікація виявленого сигналу (дружній або небезпечний) і занесення результатів в базу даних.

Радіомоніторинг забезпечує безперервність отримання, достовірність і актуальність добування даних. Безперервність досягається постійністю роботи засобів моніторингу, достовірність - документальним характером інформації, що надходить, актуальність - своєчасністю отримання необхідних для прийняття рішення даних.

В якості основних засобів радіомоніторингу використовується **автоматизований пошуковий програмно-апаратний комплекс (ПАК) DigiScan (або сучасний аналог ПАК Delta)** в складі:

- портативний комп'ютер;
- спеціальне програмне забезпечення DigiScan -2000;
- скануючий приймач AR -3000 А .

В якості додаткових засобів радіомоніторингу для пошуку джерел радіовипромінювань використовуються:

- багатофункціональний пошуковий прилад ST 031 «Піранья» в режимі високочастотного детектора-частотоміра - для локалізації місця розташування ЗП;
- індикатор поля PROTECT 1203 - для виявлення активних ЗП, впроваджених в предмети інтер'єру, а також для виявлення ЗП на рухомих об'єктах;
- портативний частотомір RFM-32 - для попередньої оцінки радіоелектронної обстановки на контрольованій території, порівняння рівнів сигналів усередині і зовні об'єкта, що перевіряється, а також для виявлення активних ЗП, впроваджених в предмети інтер'єру, а також для виявлення ЗП на рухомих об'єктах.

6.1.1. Сканування радіочастотного діапазону, аналіз радіоелектронної обстановки в приміщенні, виявлення радіовипромінювальних ЗП за допомогою ПАК DigiScan .

Автоматизований пошуковий програмно-апаратний комплекс ПАК DigiScan , що складається з портативного комп'ютера, зі спеціального програмного забезпечення DigiScan -2000 і скануючого приймача AR 3000 А,

призначений для виявлення радіосигналів з закладних пристроїв, визначення їх частоти, смуги пропускання, дослідження сигналів по кореляційних функціях, амплітудних і спектральних характеристиках, виявлення гармонік сигналу, класифікації виявленого сигналу (дружній або небезпечний) і занесення результатів в базу даних.

Порядок розгортання, включення комплексу представлений в додатку 2 цієї методики.

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

- динамічний поріг;
- вимір смуги сигналу;
- перевірка наявності гармонік сигналу;
- пасивна кореляція;
- пасивна кореляція з зондуванням;
- активна амплітудна кореляція;
- активна спектральна кореляція;
- відбір сигналів по сумарному рівню небезпеки.

Після включення ПАК для сканування діапазону частот оператор повинен виставити наступні параметри:

- 1) рівень порога і атенюатора для кожного відрізка діапазону частот;
- 2) параметри роботи приймача: для AR -3000 А рекомендується швидкість обміну 9600 бод. інтервал опитування 25 мс, кількість запитів 2;
- 3) параметри пошуку: перевіряється діапазон, крок основний панорами, поріг небезпеки (рекомендовані значення: 20 - 2036 МГц; 180 кГц; 2 - відповідно);
- 4) параметри аналізу:
 - необхідність додаткового тестування сигналів в модуляції АМ;
 - перевіряються гармоніки (рекомендується перевіряти 2-гу і 3-тю гармоніки);
 - кореляція: пасивна, пасивна з зондуванням (для скритності перевірки) або активна (рекомендується використовувати, коли можна демаскувати пошукові заходи);
- 5) параметри звуку:
 - включити параметр «Автоматичне регулювання посилення»;
 - озвучування: при пасивної кореляції виставити параметр «Немає», при активній CD - або MIDI -програвач;
 - запис звукового зразка небезпечних сигналів - 3 с;
- 6) параметри оповіщення:
 - сигналізація про закладення: виставити прапорець «При виявленні»;
 - звуковий сигнал: вибрати короткий waf -файл.

DigiScan -2000 працює в двох режимах: Пошук і Ручний режим.

Після виставлення параметрів оператор включає режим автоматичного сканування в заданому діапазоні (команда «Пошук» в меню «Режим»).

У режимі пошуку програма автоматично сканує заданий діапазон, знаходить сигнали, що перевищують заданий поріг, і виконує тести, які встановив оператор. Якщо виявлений небезпечний сигнал, програма оповіщає оператора звуковим сигналом або виводить повідомлення на екран і включає запис звукового зразка. Сигнал заноситься в розділ бази даних «Небезпечні». Всі інші сигнали заносяться в розділ бази даних «Нові». В розділ «Все» потрапляють всі сигнали, незалежно від небезпеки. Після декількох сканувань всього діапазону оператор зупиняє пошук і переходить в ручний режим.

В ручному режимі оператор може проаналізувати результати пошуку або спробувати самостійно знайти нові сигнали. Для цього оператор крокує по діапазону і виконує тести над виявленими сигналами. В ручному режимі також використовується поріг, що задається оператором. В ручному режимі оператор може переглядати осцилограму і спектр сигналів на дисплеях «Амплітуда» і «Спектр».

Алгоритм пошуку небезпечних сигналів.

Алгоритм пошуку небезпечних сигналів зображений на блок-схемі, представленої на рис. 4. Виконувана поточна операція відображається в рядку статусу внизу програми.

Сканування в основній панорамі. У режимі пошуку DigiScan -2000 починає сканування в головній панорамі. Модуляція приймача - WFM, крок сканування дорівнює смузі цієї модуляції. Для AR 3000 А ця величина складає 180 кГц. Синя вертикальна лінія на основній панорамі - це маркер, який показує поточну частоту. На головній панорамі червоною лінією відображається поріг. При перевищенні порогу програма запам'ятовує частоту, на якій почалося перевищення (F_1) і продовжує сканування до частоти, на якій перевищення закінчується (F_2). Програма запам'ятовує ці частоти і переходить до докладного сканування в допоміжній панорамі.

Основна панорама дозволяє відображати від 0.1% до 100% від перевіреного діапазону. Для збільшення або зменшення використовується регулятор в нижній лівій частині основної панорамі. Перед початком пошуку, коли буде здаватися поріг, рекомендується встановити масштаб 50-100% для перегляду всього діапазону.

Редагування порога здійснюється до початку пошуку за допомогою команди «Поріг» пункту меню «Режим».

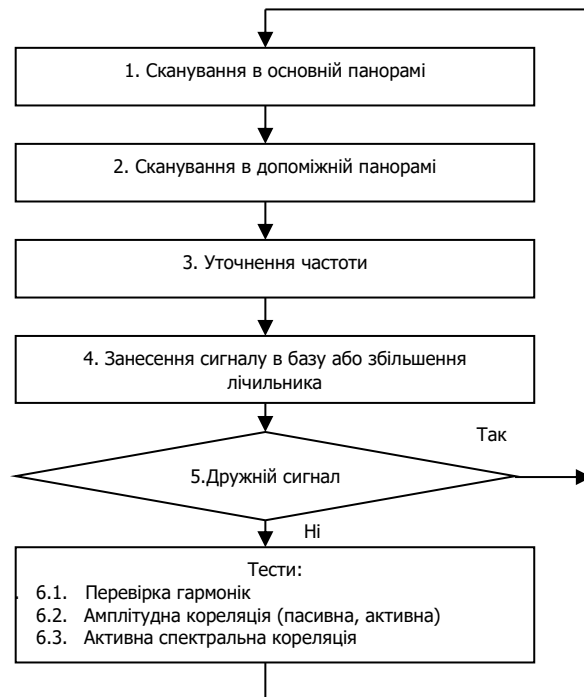


Рис. 4. Блок-схема алгоритму пошуку

Сканування в допоміжній панорамі . Модуляція приймача - NFM , крок сканування дорівнює смузі цієї модуляції. Для AR 3000 А ця величина складає 12 кГц. Маркер поточної частоти відображається синьою вертикальною лінією. Діапазон сканування в допоміжній панорамі (f_1, f_2) автоматично обчислюється за значеннями частот F_1 і F_2 :

- початок діапазону $f_1 = F_1 - 90$ кГц;
- кінець діапазону $f_2 = F_2 + 90$ кГц.

Після того, як програма закінчить сканування в діапазоні від f_1 до f_2 , вона переходить до пошуку перевищень порога. На малюнку позначені цифрами 1-4 перші чотири перевищення порога.

Виявлені сигнали програма заносить в список, вибирає перший сигнал з цього списку і переходить в режим уточнення частоти цього сигналу.

Допоміжна панорама дозволяє відображати від 0.1% до 100 від перевіреного діапазону. Для збільшення або зменшення використовується регулятор в нижній лівій частині основної панорами.

Уточнення частоти . В цьому режимі DigiScan-2000 уточнює частоту сигналу зі списку, отриманого під час детального сканування. Сканування в допоміжній панорамі проводилося з кроком, рівним смузі NFM – 12 кГц. Закладка може мати частоту, зміщену щодо 12кГц сітки і програма може неточно налаштуватися і пропустити її. Щоб уникнути цього, програма перевіряє рівень сигналу на частоті, меншою на половину кроку NFM і більшою на половину кроку NFM. Якщо на якійсь з цих сусідніх частот рівень вище, ніж на центральній частоті, то ця сусідня частота буде вважатися частотою сигналу. Таким чином, точність вимірювання частоти підвищується до 6 кГц.

Занесення сигналу в базу або збільшення лічильника . Виявлені сигнали автоматично заносяться програмою в базу даних, незалежно від рівня небезпеки. Якщо сигнал уже є в базі даних, його лічильник збільшується на 1.

Пропуск дружніх сигналів . Якщо сигнал уже є в базі даних і позначений як дружній, то процес пошуку пропускає цей сигнал і продовжує роботу по перевірці інших сигналів або скануванню. Дружні сигнали мають позначку "ДР" біля рівня небезпеки. При роботі в ручному режимі позначку "Др" потрібно ставити вручну.

Примітка. Позначка сигналів як "дружніх" виключає їх з тестування під час пошуку. Необхідно точно впевнитися, що всі сигнали безпечні, інакше можна пропустити закладку.

Перевірка гармонік . В цьому режимі DigiScan-2000 перевіряє наявність 2-ї і 3-ї гармоніки сигналу. Через обмеження в обсязі і потужності закладки, а також близькості до її антени, сигнал може мати гармоніки, кратні основній частоті. Наявність гармонік підвищує рівень небезпеки сигналу.

Знаючи основну частоту сигналу, програма обчислює частоти гармонік, множачи основну частоту на 2 (2-га гармоніка) і на 3 (3-тя гармоніка). Після цього на приймачі встановлюється модуляція WFM , він налаштовується на частоти гармонік, і проводиться зчитування рівня на цих частотах. Якщо

рівень сигналу на цих частотах перевищує поріг, то вважається, що частота має гармоніки.

Якщо частота має обидві гармоніки, то сумарний рівень небезпеки сигналу підвищується на 1. Якщо гармонік немає або є одна з двох, то рівень небезпеки не підвищується.

Якщо налаштуватися на частоту гармоніки в ручному режимі, то можна почути такий же звук як на основній частоті, тільки з деякими спотвореннями.

Для повноти аналізу рекомендується завжди встановлювати перевірку гармонік. Якщо діапазон перевірки починається з частоти вище 1000 МГц, то перевірка 3-ї гармоніки не має сенсу, тому що частота 3-ї гармоніки буде вище верхнього діапазону приймача. При накопиченні бази даних дружніх сигналів рекомендується відключати перевірку гармонік.

Амплітудна кореляція .

У цьому режимі програма вимірює зв'язок між акустикою, приміщенням що перевіряється і сигналом на звуковому виході приймача, який називається кореляцією (К). При амплітудній кореляції йде порівняння амплітуди сигналу в часі. Для аналізу акустики приміщення використовується активний референтний мікрофон, що входить в комплект комплексу. Кореляція (коефіцієнт кореляції) може перебувати в діапазоні від -1 до +1. Якщо зв'язок між акустикою приміщення і сигналом на виході приймача є, то кореляція буде близька до +1. Така кореляція говорить про те, що приймач налаштований на закладний пристрій.

У режимі пошуку амплітудна кореляція проводиться при декількох видах модуляції - WFM, NFM і AM (встановлюється перед включенням режиму пошуку).

Результати вимірювання кореляції відображаються в правій нижній частині головного вікна DigiScan -2000 на сторінці «Протокол». Амплітудна кореляція позначається К 1. У базу даних потрапляє максимальне значення кореляції при модуляції WFM, NFM і AM і зберігається в полі К 1.

У відповідності зі значенням К1 обчислюється рівень небезпеки перевіреного сигналу:

- при $K1 = 0-0,33$, рівень небезпеки не змінюється;
- при $K1 = 0,33-0,66$, рівень небезпеки підвищується на 1;
- при $K1 = 0,66-1,0$, рівень небезпеки підвищується на 2.

Залежно від умов, в яких проводиться перевірка, *можна використовувати один з видів амплітудної кореляції:*

- пасивна
- пасивна з зондуванням
- активна

Пасивна кореляція. Пасивна кореляція проводиться беззвучно і не демаскує пошукове заход. Для успішного проведення пасивної кореляції в приміщенні повинен бути якийсь звук. Це може бути музика з CD - або MIDI - програвач комп'ютера, запис курсу англійської мови на касеті або радіоприймач. Якщо використовується радіоприймач, то частота, на яку він налаштований, може бути занесена програмою в розділ

«Небезпечні». Пасивна кореляція дає менш точні результати, ніж активна. Наприклад, якщо в активному режимі кореляція закладки дорівнює 0.76, то в пасивному вона може бути 0.45, а іноді і менше. Якщо кількість проходів діапазону більше одного, то ймовірність пропуску небезпечного сигналу зменшується. Для підвищення точності вимірювання пасивної кореляції необхідно ставити час кореляції більший, ніж при проведенні активної. Для пасивної кореляції рекомендується виставляти час не менш як 10 сек.

Для озвучування приміщення можна використовувати CD - або MIDI - програвач комп'ютера. Установка цих параметрів виконується на сторінці «Звук» команди «Параметри» в меню «Режим».

Пасивна кореляція з зондуванням. Той же тест, що і пасивна кореляція, за винятком того, що програма під час вимірювання кореляції періодично змінює гучність CD - або MIDI -програвача. Спочатку гучність стає максимальною, потім мінімальною і т.д. Це дозволяє значно підвищити точність кореляції і не демаскувати процес пошуку. Суб'єкт, який прослуховує може подумати, що просто йде настройка гучності. Такий вид кореляції вимагає використання озвучування за допомогою CD - або MIDI -програвача комп'ютера. Час пасивної кореляції з зондуванням може бути 5-10 с.

Активна амплітудна кореляція. Під час активної амплітудної кореляції DigiScan -2000 також порівнює амплітуду акустики приміщення і сигналу з звукового виходу приймача. Відмінність полягає в тому, що під час активної кореляції колонки комп'ютера відтворюють звукові імпульси, які значно підвищують точність і надійність пошуку. Звукові імпульси відтворюються з випадковим періодом від 0.2 до 1 с. При використанні активної кореляції час може бути меншим (3-5 с), хоча для підвищення надійності можна встановити і більшим.

Спектральна кореляція. У цьому режимі програма порівнює спектр акустики приміщення і сигналу з звукового виходу приймача. Для успішного проведення спектральної кореляції необхідно, щоб в приміщенні звучав сигнал з частотою, що змінюється. Це досягається відтворенням звукового файлу default . wav з таким сигналом. Час кореляції залежить від довжини цього файлу.

Спектральна кореляція також проводиться при декількох видах модуляції - WFM , NFM і АМ . Результати спектральної кореляції відображаються в закладці «Аналіз» головного вікна в колонці К 2. Таке ж ім'я має поле бази даних, в якому зберігається максимальний результат кореляції (при різній модуляції).

Коли спектральна кореляція близька до -1, це означає що є зворотний зв'язок між спектром звуку в приміщенні і спектром сигналу. Це можливо при використанні радіопередавачів з інверсією спектру.

У відповідності зі значенням К2 обчислюється рівень небезпеки перевіреного сигналу:

- при $K2 = 0-0.33$, рівень небезпеки не змінюється;
- при $K2 0,33-0.66$, рівень небезпеки підвищується на 1;

- при $K_2 = 0,66-1,0$, рівень небезпеки підвищується на 2.

Загальний рівень небезпеки сигналу обчислюється за наявності гармонік і за коефіцієнтами амплітудної і спектральної кореляції. При перевищенні рівня небезпеки порогового значення (рекомендоване значення 2), сигнал класифікується як небезпечний і заноситься в базу небезпечних сигналів.

Аналіз результатів пошуку. Після декількох проходів і сканування заданого діапазону частот можна роздрукувати всю базу або базу даних небезпечних сигналів, в якій записані такі параметри сигналів:

- частота, модуляція, смуга;
- наявність гармонік;
- значення K_1 і K_2 ;
- загальний рівень небезпеки;
- час, дата занесення сигналу в базу;
- значення лічильника (скільки разів сигнал зустрічався в процесі пошуку);
- коментар.

База даних має наступні розділи: «Нові», «Небезпечні», «Дружні», «Все».

Після цього детально аналізуються *всі небезпечні сигнали в ручному режимі*:

- прослуховується небезпечний сигнал;
- записується сигнал в waf -файл;
- аналізується осциллограмма;
- аналізується спектрограмма;
- прослуховуються 2-а і 3-я гармоніки;
- обчислюється коефіцієнт амплітудної кореляції;
- обчислюється коефіцієнт спектральної кореляції.

На основі детального аналізу небезпечних сигналів *робиться висновок* про наявність в приміщенні, що перевіряється радіовипромінювальних закладного пристрою і його характеристиках.

Всі результати роботи автоматично заносяться в файл протоколу, який є звітним документом. Роздруківка протоколу додається до акта перевірки (дод. б). Крім того, до звітних документів відносяться база небезпечних сигналів, осцилограми, спектрограми сигналів виявлених закладних пристроїв.

Локалізація та пошук місця розташування виявлених радіопередавальних ЗП виконується за допомогою додаткових пошукових засобів:

- ST 031 « Піранья »;
- PROTECT 2103;
- RFM -32.

6.1.2. Локалізація місця розташування радіовипромінювальних ЗП за допомогою пошукового приладу ST 031 «Піранья».

Багатофункціональний пошуковий прилад ST 031 «Піранья» призначений для проведення заходів з виявлення та локалізації спеціальних технічних засобів негласного знімання інформації, для виявлення природних і штучно створених каналів витоку інформації, а також для контролю якості захисту інформації. Він забезпечує рішення контрольних-пошукових завдань тільки в межах приміщення (об'єкта) або в безпосередній близькості до нього.

Детальний опис приладу ST 031 «Піранья», підготовка його до роботи, перевірка працездатності і рекомендації щодо його використання наведені в додатку 3.

Виявлення факту роботи (виявлення) і локалізація місця розташування радіовипромінювальних ЗП, що створюють потенційно небезпечні, з точки зору витоку інформації, радіовипромінювання здійснюється в режимі високочастотного детектора-частотоміра (RADIO FREQUENCY CHANNEL).

Ефективність застосування приладу ST 031 «Піранья» для проведення контрольних-пошукових робіт визначається: ступенем підготовленістю оператора до використання приладу; повнотою і якістю підготовчих заходів; відповідністю порядку дій оператора загальними правилами і апробованим на практиці прийомів.

Оператор повинен мати стійкі навички підготовки, перевірки та управління приладом в передбачених режимах, а також навички аналізу результатів слухового і візуального (за осцилограмами і спектрограмами) контролю параметрів потенційно небезпечних сигналів.

Особливості режиму високочастотного детектора-частотоміра.

У цьому режимі прилад забезпечує прийом радіосигналів в діапазоні від 30 до 2500 МГц в ближній зоні (в межах об'єкта спецробіт), їх детектування і висновок для слухового контролю і аналізу у вигляді змінних тональних посилок (клацань), або у вигляді явних фонограм при їх прослуховуванні як на вбудований гучномовець, так і в навушниках.

У кожен конкретний момент часу на тлі реальної завадної обстановки приймається і детектується найбільш потужний з усіх радіосигналів в робочому діапазоні. Його рівень, щодо встановленого порогу детектора, відображається на дворядковому індикаторі з 40-сегментною шкалою у верхній частині рідкокристалічного дисплея.

Різниця в використанні двох шкал полягає в наступному: верхня шкала відображає середні значення продетектованого сигналу, а нижня його пікові значення. Відповідно, у верхньому рядку будуть переважати сигнали з постійною частотою (без модуляції, частотномодульовані), а в нижній близькі до імпульсних видів сигналів (наприклад сигнали з амплітудною і імпульсною модуляцією). Наявність індикації на двох шкалах говорить про змішаному вигляді сигналу на вході детектора (наприклад, телевізійного сигналу).

У разі впевненого прийому сигналу зі свідомо відомими параметрами відображається напис ідентифікації сигналу під цифровою шкалою рівня сигналу.

Можлива індикація виявлення сигналів наступних стандартів: GSM (напис « GSM »), DECT (напис « DECT »).

Залежно від умов і цілей проведення контрольних-пошукових робіт є можливість вибору і установки необхідного (найбільш раціонального) порогу детектора.

Одночасно здійснюється вимір поточних значень частоти прийнятого радіосигналу і визначення найбільш стійкого її значення (для сигналів з постійною частотою). І ті, і інші значення в явному вигляді відображаються на екрані дисплея.

Для якісної оцінки ступеня мінливості частоти радіосигналу використовується спеціальна обчислювальна процедура, результати якої відображаються на екрані дисплея у вигляді тонкої горизонтальної лінії, що динамічно змінюється в довжині безпосередньо над цифровими символами поточних значень частоти. Довжина лінії пропорційна до похідної від частоти прийнятого сигналу.

Підготовка контрольованого приміщення.

Закрити двері і вікна, а також штори або жалюзі. Для зменшення фону електричного поля потрібно вимкнути оргтехніку, мережеві адаптери, трансформатори, радіотелефони, люмінесцентні освітлювальні лампи і інші електронні пристрої та електроприлади - потенційні джерела підвищення фону. Перевірку цих пристроїв слід проводити окремо, включаючи їх по черзі. Якщо перевіряється приміщення або суміжні приміщення, обладнані системами активного радіотехнічного маскування (радіочастотні генератори шуму і т.п.), їх необхідно вимкнути на час проведення перевірки.

Для активації телефонних радіозакладок рекомендується зняти трубки телефонів.

Для активації радіозакладок з акустичним пуском і забезпечення класифікації виявлених радіосигналів, потрібно включити ідентифікаційне джерело звуку, в якості якого можна використовувати магнітофон або CD-плеєр в режимі відтворення музики або мовної фонограми. Не рекомендується використовувати в цих цілях радіоприймач або телевізор, так як звуковий сигнал, який створюється ними може корелювати з відповідним радіосигналом, на якому ведеться дана передача, прийнята приладом ST 031.

Візуально визначити потенційно небезпечні місця, з яких доцільно почати перевірку (стіл переговорів, робочий стіл та інші місця найбільш ймовірного розміщення радіозакладок).

Включення приладу ST 031 в режим високочастотного детектор-частотоміра здійснюється в наступному порядку:

- переконатися в тому, що прилад вимкнений («POWER» - «OFF»);
- звільнити роз'єми основного блоку управління, обробки та індикації «RF ANT» і «PROBES» від додаткових зовнішніх пристроїв;
- до гнізда «RF ANT» підключити телескопічну антену (через

перехідник) або високочастотну антену;

- включити живлення приладу: перемикач «POWER» - «ON»;
- одночасно з мелодійним сигналом включиться підсвічування РК дисплея і на ньому з'явиться напис «RADIO - FREQUENCY», «CHAN NEL», «30 ... 2500 MHz».

Примітка. Не допускається одночасна робота ST 031 «Піранья» з нелінійним локатором.

Порядок управління приладом в режимі високочастотного детектора-частотоміра.

Установка «нульового» порогу детектора здійснюється при включенні автоматично. У разі необхідності, натисканням кнопок «<» або «>» встановити поріг детектора вручну, керуючись показаннями додаткової шкали «min - - - | - - -max». Якщо буде потрібно, натисканням кнопки «□» повернутися до автоматичної установки порога.

Візуально за кількістю повністю забарвлених елементів індикаторів рівня сигналу і «на слух» по частоті клацань у вбудованому гучномовці або навушниках оцінити рівень сигналу.

При необхідності натисканням кнопки «SET» встановити необхідні значення динамічного діапазону: (8 - 16) дБ; (8 - 32) дБ; (8 - 48) дБ.

Натиснути кнопку «RUN / STOP» і зупинити (при необхідності) динамічні вимірювання рівня і частоти радіосигналу. Повторним натисканням цієї кнопки відновити динамічні виміри.

Натиснути кнопку «ENTER» (переклад звукової індикації в режим «A U D»), прослухати наявність і зміст потенційно небезпечних модульованих радіовипромінювань.

Натисканням кнопок «+» і «-» встановити необхідну гучність виведеного або на вбудований гучномовець, або на навушники звукового сигналу (тонального або демодульованого).

Натиснути кнопку «OSC» і перейти (при необхідності) до Осцилографічного контролю параметрів сигналу.

Натиснути кнопку «SA» і перейти (при необхідності) до аналізу спектра демодульованого сигналу.

У разі збоїв в роботі натиснути кнопку «RESET» та здійснити перезапуск приладу.

Установка порога чутливості приладу ST 031.

Підготовка самого приладу ST 031 «Піранья» (після перевірки його працездатності в даному режимі) полягає в установці «нульового» порогу детектора, що є, фактично, визначальним для успішного проведення робіт. Зниження порогу обов'язково призведе до частих помилкових спрацьовувань індикації, а його завищення - до ймовірного пропуску сигналу ЗП. І те, і інше значно ускладнює роботу оператора, збільшує час і знижує вірогідність результатів перевірки. Тому для установки «нульового» порогу необхідно обов'язково дотримуватися кількох простих правил.

Не можна проводити установку порога в приміщенні, що перевіряється, так як при функціонуванні в ньому вже розміщеної

радіозакладки, рівень її радіовипромінювання буде визначено приладом як «нульовий».

Неприпустимо використання радіостанцій, радіотелефонів і інших радіовипромінювальних засобів в процесі налаштування порогу.

Не наближати антену приладу до включених ПЕОМ та інших засобів оргтехніки, як джерел ПЕМІ в діапазоні роботи приладу.

Не допускати контакту антени приладу з металевими предметами і проводами, як джерелами перевипромінювання високочастотних сигналів.

Налаштування приладу слід проводити в одному з найближчих до приміщення, що перевіряється, в якому, імовірно, рівень фону істотно не відрізняється, а установка «радіозакладок» або неможлива, або недоцільна. У якості таких приміщень зазвичай розглядають приміщення іншого призначення, але розташовані на тому ж поверсі і з віконними прорізами, що виходять на ту ж сторону будівлі.

Якщо об'єктом перевірки є автомобіль або інший рухомий об'єкт, то налаштування «нульового» порогу слід проводити не ближче 10 - 20 метрів від нього.

Після установки «нульового» порогу прилад переміщують в контрольоване приміщення (до контрольованого об'єкту) БЕЗ ВІДКЛЮЧЕННЯ ЖИВЛЕННЯ. Бо кожне наступне його включення призводить до автоматичної установки порога вже відповідно до нових умов електромагнітної обстановки.

Виконавши викладені вище правила і обмеження, можна вважати, що приміщення, яке перевіряється (об'єкт) і прилад ST 031 «Піранья» підготовлені до проведення контрольно-пошукових робіт.

При проведенні пошукових робіт застосовуються два методи пошуку:

- амплітудний метод пошуку;
- метод пошуку «акустичної зав'язки».

Амплітудний метод.

Цей метод заснований на різкому зростанні рівня прийнятого сигналу і при розміщенні прийомної антени приладу в ближній зоні джерела.

Величина радіусу виявлення локального джерела залежить від потужності випромінюваного ним сигналу, діаграми спрямованості і орієнтації його антени та рівня фону електричного поля в точці розташування приймальної антени.

Виявивши небезпечний радіосигнал, необхідно рухатися в напрямку зростання його рівня. Контроль за рівнем сигналу здійснюється за шкалою індикації рівня і збільшення частоти клацань звукової сигналізації в режимі «TONE». При фарбуванні всіх сегментів шкали індикації рівня, необхідно збільшувати її діапазон кнопкою «SET», а також збільшувати поріг виявлення кнопкою «<».

Метод «акустичної зав'язки».

Цей метод заснований на виникненні позитивного акустичного зворотнього зв'язку між мікрофоном радіозакладки і динаміком приладу ST 031. Для використання даного методу необхідно включити режим

«AUD». Акустична зав'язка може виникнути тільки в разі виявлення мікрофонної радіозакладки, в якій використовуються звичайні види амплітудної і частотної модуляції, і на виході амплітудного детектора ST 031 прослуховується акустичний фон приміщення. При виникненні акустичної зав'язки динамік приладу видає характерний «писк», тон і інтенсивність якого змінюються при наближенні до джерела (мікрофону радіозакладки).

Дальність виникнення ефекту акустичної зав'язки залежить від гучності звуку, видаваного динаміком приладу ST 031. Зменшуючи гучність кнопкою «-» і скорочуючи область виникнення акустичної зав'язки, можна домогтися точної локалізації джерела.

Слід враховувати, що виникнення характерного звуку при використанні даного методу демаскує проводяться роботи і, при наявності в радіозакладці пристрою дистанційного керування, вона може бути виключена або перебудована на іншу частоту.

Особливості пошуку радіовипромінювальних ЗП за допомогою пошукового приладу ST 031.

Радіочастотний канал приладу ST 031 являє собою широкосмуговий приймач прямого підсилення з амплітудним детектором, вбудованим частотоміром і широкодіапазонною виносною антеною. Принцип виявлення радіосигналів за допомогою нього полягає в посиленні, детектуванні і визначенні частоти наведених в антені електромагнітних хвиль, інтенсивність яких перевищує порогове значення (рівень фону). Ознаками виявлення радіосигналу є:

- фарбування позитивних сегментів (правіше нуля) на шкалі індикації рівня. Чим більше рівень наведеного сигналу, тим більше забарвлених сегментів;
- відносно стабільне значення частоти. Межі коливання значення частоти можуть бути від десятих до декількох сотих кілогерц і залежать від стабільності несучої частоти передавача, виду модуляції сигналу, рівня сигналу, наведеного в антені. Для зручності оцінки стабільності прийнятої частоти над рядком Freq = ****. ** виводиться тонка горизонтальна лінія, довжина якої пропорційна модулю похідної від частоти (чим стабільніша частота сигналу, тим коротша лінія). При збігу значень декількох вимірювань частоти, фіксується факт захоплення частоти появою на дисплеї напису Capt = ****. ** MHz, з втратою частоти цей напис зникає;
- поява клацань звукової сигналізації в режимі «TONE» при перевищенні рівня сигналу над порогом більш ніж на чотири сегменти. Із зростанням рівня частота клацань збільшується;
- стабільне прослуховування демодульованого сигналу в режимі «AUD».

В результаті численних перевідбиттів і перевипроміненнь електромагнітних хвиль зовнішніх і внутрішніх джерел в контрольованому приміщенні формується складна картина розподілу максимумів і мінімумів напруженості електричного поля. Це призводить до спрацьовування індикації приладу не тільки в разі виявлення сигналу радіозакладки. У зв'язку з цим всі

виявлені сигнали необхідно класифікувати для оцінки ступеня їх небезпеки і визначати місце розташування джерела (зовнішнього, внутрішнього).

Небезпечні сигнали:

а) сигнали радіозакладок - джерело може бути внутрішнім або зовнішнім. Внутрішній - радіозакладка встановлена в приміщенні, що перевіряється. Зовнішній - радіопередавач встановлений за межами приміщення, але в зоні прийому його приладом ST 031, наприклад:

- радіомікрофон з виносним мікрофоном;
- винесений радіопередавач прихованої відеокамери;
- радіостетоскоп, встановлений із зовнішнього боку стіни;
- телефона радіозакладка, встановлена на лінії зв'язку за межами приміщення, але в безпосередній близькості до нього;

б) сигнал просторового високочастотного нав'язування - зондуєчий сигнал - зовнішній, перевідбитий - внутрішній;

в) сигнали ПЕМІ від ПЕОМ, факсів та інших електронних приладів і пристроїв - можуть бути досить потужними і, при використанні зацікавленими особами спеціальної приймальної апаратури, можливе перехоплення конфіденційної мовної, комп'ютерної і передаваної по каналах зв'язку інформації. Сигнали ПЕМІ - внутрішні.

Безпечні сигнали:

а) сигнали від зовнішніх джерел (ШМРС, ТВР, засобів радіозв'язку та ін.) - класифікуються "на слух" в режимі «AUD». Відзначаються з найбільшим рівнем поблизу вікон, в кутах приміщення, поблизу внутрішніх перевипромінюючих і перевідбиваючих об'єктів і поверхонь (великі металеві предмети і поверхні, корпусу ПЕОМ, сейфи, батареї опалення, трубопроводи, дроти). Стабільність частоти - низька;

б) сигнали від внутрішніх джерел (електроприладів, оргтехніки, блоків живлення) - при прослуховуванні в режимі «AUD» не містять ознак модуляції акустикою приміщення і цифрової передачі. У режимі осцилографа («OSC») демодульований сигнал має частоту 50 Гц (або гармоніки). Відзначається в безпосередній близькості від джерела.

Особливості радіовипромінювальних різних ЗП, що використовують радіочастотний канал передачі, описані в додатку 3.

Після виявлення і локалізації місця розташування впроваджених ЗП необхідно приступити до фізичного пошуку і знешкодження ЗП. Результати пошуку в обліковій та звітній документації (дод. 6). При фізичному пошуку впроваджених в предмети інтер'єру ЗП можна також застосовувати детектор поля PROTECT 1203 або частотомір RFM -32.

6.1.3. Пошук і виявлення активних радіовипромінювальних ЗП за допомогою детектора поля PROTECT 2103.

Детектор поля PROTECT 1203 призначений для пошуку і виявлення закладних пристроїв, коли вони знаходяться в активному режимі. За допомогою PROTECT 1203 можна перевіряти приміщення, машини, різні

предмети інтер'єру, а також людей на предмет наявності ношених передавачів. Пошук здійснюється і в прихованому режимі, для чого використовується вбудований в прилад вібратор. Прилад визначає наявність у співрозмовника працюючого мобільного телефону. Детальний опис приладу наведено в додатку 5 до цієї Методики.

Пошук активних ЗП в приміщеннях.

Необхідно закрити всі вікна і штори в приміщенні. Увімкнути освітлення та офісне обладнання для створення нормальних умов роботи. Перш ніж входити в приміщення, що перевіряється необхідно включити прилад і витягти антену на середню довжину. Необхідно переконатися, що висунутий перший (найширший) сегмент антени. Можна заховати інші сегменти антени, але перший сегмент повинен бути висунутий.

Налаштування чутливості приладу. Для цього ручка налаштування викручується до тих пір, поки не буде світитися або блимати тільки один сегмент на світлоіндикаторі. Якщо під час пошуку оператор не хоче, або не має можливості спостерігати рівень радіополя за допомогою світлоіндикатора, то можна встановити чутливість, при якому горять всі зелені сегменти. В цьому випадку, якщо оператор наблизиться до джерела випромінювання, будуть світитися червоні сегменти і включитися вбудований вібратор.

Алгоритм пошуку активних ЗП заснований на амплітудному методі і включає наступні операції:

1. Увійти в приміщення, що перевіряється тримаючи детектор вертикально і спостерігаючи світіння світлоіндикатора. Включити і вимкнути світло, офісне обладнання та інші електроприлади. Спостерігати зміни показань приладу. Якщо вони змінюються синхронно з позначкою включення / вимкнення будь-якого обладнання, то це сигнал про можливу наявність в цьому приладі закладного пристрою несанкціонованого зйому інформації.

2. Обійти всю кімнату, спостерігаючи показання приладу. При наближенні / видаленні до джерела випромінювання буде відповідно збільшуватися / зменшуватися показуваний рівень випромінювання.

3. Визначити місце з найбільшим рівнем випромінювання, переміщаючи прилад у всіляких напрямках і спостерігаючи свідчення світлоіндикатора.

4. Перевірити всі предмети, які можуть містити заставні перші пристрої. Сигналом про виявлення подібного роду передавачів є зміни показань світлового індикатора.

5. Необхідно точно визначити місцезнаходження джерела нелегального випромінювання. Для цього потрібно зменшити до мінімуму чутливість приладу. Якщо антена висунута в повному обсязі, то рівень радіополя, що відображається на світловому індикаторі, не буде залежати від взаємного розташування антени і передавача, і можна спостерігати постійний рівень випромінювання поблизу передавача. Іноді світлоіндикатор може показати збільшення рівня радіополя поблизу проводів або металевих об'єктів. Це пов'язано з тим, що металеві об'єкти виступають як «продовження» антени і такі ситуації не обов'язково сигналізують про наявність передавача.

6. Після виявлення точного місцезнаходження джерела випромінювання необхідно приступити до фізичного пошуку. Провести візуальний огляд і перевірку з допомогою детектора кожного об'єкта, що знаходиться в "небезпечній" зоні. При необхідності - розібрати освітлювальні прилади, телефон, розетки електроживлення, телефонні розетки датчики пожежної сигналізації і т.д. Дуже ретельно оглянути телефонні лінії і лінії електроживлення 220 В. Оглянути всі предмети інтер'єру, книги, вміст столів і т.д.

7. Якщо виявлено закладний пристрій, то подальший пошук не припиняється. Необхідно гранично уважно продовжувати пошук, так як немає ніякої гарантії, що в приміщенні, що перевіряється впроваджено тільки один ЗП. Професіонали часто "ставлять" 2 пристрої прослуховування - один доволі легко виявляється, а другий добре замаскований, з дистанційним управлінням, з нестандартною модуляцією і т.д.

Перевірка телефонних ліній.

Телефонний жучок може бути встановлений на будь-якому відрізьку телефонної лінії: в телефонному апараті, телефонній розетці, комутаційній коробці або на телефонному кабелі. Більшість телефонних жучків активізується тільки при піднятті трубки, тому перевірка виконується при піднятій трубці.

Слід починати перевірку з телефонного апарату. Антену детектора розмістити біля апарату і підняти трубку. Спостерігати зміни рівня радіополя. Якщо перевіряється радіотелефон, то, природно, буде виявлено сильне збільшення рівня радіополя при знятті трубки з бази, внаслідок того, що трубка і база зв'язуються по радіоканалу. Слід зазначити, що радіотелефон сам по собі є прекрасним радіовипромінювальним жучком.

Для подальшого пошуку ЗП необхідно переміщати антену детектора уздовж телефонної лінії при піднятій трубці. Перевірити всі розетки і комутаційні коробки. У процесі перевірки телефонних ліній, розеток варто кілька разів підняти і покласти трубку телефонного апарату. Якщо буде помічено, що рівень радіополя змінюється синхронно з підняттям / опусканням трубки, то можна зробити висновок про наявність на лінії телефонного закладного пристрою. Потім необхідно визначити ділянку лінії з максимальним рівнем випромінювання і провести ретельний фізичний пошук.

Перевірка людей на наявність радіовипромінювальних ЗП.

Існує велика кількість передавачів, вбудованих в одяг, особисті речі відвідувача і т.д. Ці пристрої можуть транслювати переговори або (і) відеоінформацію. Для перевірки необхідно налаштувати чутливість таким чином, щоб світилися всі зелені сегменти світлоіндикатора. Сховати детектор поля PROTECT 12 03 в кишені або під одягом, попередньо висунувши перший (найширший) сегмент антени і включити живлення приладу. При наближенні до зловмисника, який має ЗП, включиться вбудований вібратор детектора, що сигналізує про наявність радіосигналу в приладі.

Альтернативним методом перевірки відвідувачів є розташування детектора PROTECT 1203 під столом з висунутою антеною по можливості

ближче до співрозмовника. Необхідно спостерігати зміни показань світлоіндикатора, коли відвідувач сідає за стіл або встає з-за столу.

Результати роботи інструментального контролю і пошуку ЗП детектором поля PROTECT 1203 заносяться в облікову і звітну документацію (дод. б).

6.2. Пошук закладних пристроїв, що використовують провідні комунікації

Для пошуку ЗП, які використовують провідні комунікації, застосовується багатофункціональний пошуковий прилад SWT 031 «Піранья» в режимі скануючого аналізатора провідних ліній (WIRE LINES ANALYSIS).

Цей режим призначений для пошуку і локалізації закладних пристроїв, несанкціоновано передаючих інформацію по провідних лініях (електрична мережа 220В, 50Гц, кабелі телефонних ліній, локальних обчислювальних мереж, пожежної та охоронної сигналізації і ін.). До таких закладних пристроїв відносяться:

- закладні пристрої, що використовують для передачі перехопленої інформації лінії мережі змінного струму 220В і здатні працювати на частотах до 15МГц;
- ПЕОМ та інші технічні засоби виготовлення, розмноження і передачі інформації;
- технічні засоби систем лінійного високочастотного нав'язування, що працюють на частотах понад 150кГц;
- закладні пристрої, що використовують для передачі перехопленої інформації абонентські телефонні лінії, лінії систем пожежної та охоронної сигналізації з частотою понад 20 кГц.

Підготовка приладу до роботи.

Підключіть мережевий адаптер до гнізда "PROBES".

Увімкніть прилад. На дисплеї повинен з'явитися напис "WIRE LINES ANALYSIS", що підтверджує включення режиму аналізатора провідних ліній.

Переконайтеся в працездатності приладу, використовуючи тестовий мережевий датчик. При відсутності тестового мережного датчика, ознакою справності аналізатора є прийом і детектування сигналів в електромережі 220В (наведення від мовних радіостанцій КХ і СХ діапазонів).

Для зручного підключення до лінії, що перевіряється використовуйте відповідні наконечники кабелів адаптера.

У режимі панорамного аналізу ("PANORAMA") через кнопку "SET" доступні наступні функції:

- "4" - установка початкової і кінцевої частот діапазону сканування;
- "2" - включення / вимикання режиму вирахування спектра, показаного на дисплеї до включення цього режиму, з знову вимірюваного спектра;
- "3" - включення / вимикання ручного регулювання нижнього порога індикації вимірювача рівня;
- "5" - вибір масштабу амплітудної шкали "0.1-10mV" або "0.1-1mV".

Перевірка електричної мережі 220В, 50Гц.

При підключенні приладу ST 031 до електромережі і перевірці підключених електроприладів обов'язково дотримуйтесь правил і заходів безпеки, напруга 220В є небезпечною для життя. З метою безпеки приладу, не можна підключати його до напруги більше 600 В.

Перевірку необхідно починати з мережевих розеток. Для зменшення рівня шумів в електромережі, вимкніть від електромережі (з видимим відключенням шнурів живлення від розеток) всі споживачі електричного струму і апаратуру, розміщену в контрольованому приміщенні. Підключіть наконечники приладу до електромережі, використовуючи для цього одну з розеток. Світіння двох світлодіодів на адаптері свідчить про наявність змінної напруги.

Проскануйте детально весь діапазон від 0 до 15МГц, розбивши його на інтервали. Межі інтервалів задаються кнопками "SET", "4". Ширина інтервалів визначається завантаженістю діапазону сигналами. Запуск і зупинка сканування здійснюється кнопкою "RUN / STOP". Після проходу одного або декількох циклів розгортки, оцініть рівні сигналів, що перевищують рівень шуму. Встановіть вручну необхідний поріг для автоматичної зупинки сканування на сигналі. Для цього натисніть кнопку "SET", кнопкою "3" виберіть режим "SQELCH LEVEL", потім "ENTER". Рівень порога встановлюється кнопками «Δ», «∇». Для зручності рівень порогу відображається в правій частині дисплея короткою горизонтальною лінією.

При зупинці на сигналі зробіть точне підстроювання кнопками «<», «>». Зробіть аналіз сигналу "на слух", включаючи по черзі амплітудний і частотний детектори кнопкою "ENTER".

Для аналізу слабких сигналів змініть масштаб амплітудної шкали кнопками "SET", "5" ("0.1-10мВ" або "0.1-1мВ"). Якщо сигнал має ознаки модуляції акустикою приміщення, для локалізації джерела необхідно використовувати метод акустичної зав'язки, по черзі підключаючись до всіх розеток перевіряється приміщення. З метою забезпечення безпеки, для проведення фізичного пошуку джерела небезпечного сигналу в розетках, необхідно їх знеструмити.

Після проведення аналізу виявлених сигналів збережіть в пам'яті приладу панораму кожного інтервалу натисканням кнопок: "SAVE", "ENTER".

Перевірте трійники, подовжувачі і електроприлади, по черзі підключаючи їх до електромережі.

Перевірте по черзі засоби обчислювальної та іншої техніки.

Для прискорення виявлення новозафіксованих сигналів при включенні чергового перевіряючого технічного засобу доцільно використовувати режим віднімання спектрів:

- а) викличте з пам'яті панораму, збережену раніше при перевірці розетки, до якої підключено перевіряючий пристрій, кнопкою "LOAD";
- б) встановіть режим віднімання кнопками "SET", "2";

в) запустіть сканування з параметрами, прочитаними з пам'яті, кнопкою "ENTER";

г) зробіть аналіз нових сигналів;

д) проскануйте весь діапазон частот, викликаючи з пам'яті по черзі панорами збережених інтервалів, як зазначено вище.

Перевірте освітлювальну мережу.

Слід зазначити, що за допомогою приладу ST 031 можна визначити тільки факт наявності наводок від засобів обчислювальної та іншої техніки. Визначити степінь їх інформативності (небезпеки) і зробити висновок про необхідність вжиття додаткових заходів захисту можна тільки після проведення спеціальних досліджень конкретних технічних засобів з використанням спеціальної вимірювальної апаратури.

Перевірка телефонних ліній.

Режим аналізатора провідних ліній може бути використаний для виявлення сигналів телефонних закладок, що передають акустичну інформацію приміщення на несучій частоті понад 20 кГц по дротах телефонної лінії, сигналів високочастотного лінійного нав'язування, а також факту несанкціонованого підключення мікрофона телефонного апарату (або додаткового спеціального мікрофона) до лінії при покладеній слухавці.

Для проведення перевірки необхідно підключитися до телефонної лінії голчастими накінецьниками або зажимами. Перевірку слід проводити при покладеній трубці телефону. Аналіз сигналів здійснюється так само, як при перевірці електромережі.

Перевірка систем охоронної, пожежної сигналізації та інших провідних ліній.

Всі провідні лінії, виявлені в приміщенні (в тому числі і невідомого походження - в першу чергу) необхідно по черзі перевірити. Світіння тільки одного світлодіода на адаптері приладу свідчить про наявність в лінії, що перевіряється постійної напруги.

Аналіз сигналів здійснюється так само, як при перевірці електромережі.

Результати роботи інструментального контролю приладом ST 031 в даному режимі заносяться в облікову і звітну документацію (дод. 6).

6.3. Пошук закладних пристроїв, що використовують низькочастотні магнітні випромінювання.

Для пошуку ЗП, що використовують низькочастотні магнітні випромінювання, застосовується багатофункціональний пошуковий прилад SWT 031 «Піранья» в режимі детектора низькочастотних магнітних полів (MAGNETIC CHANNEL).

Цей режим призначений для пошуку і локалізації розташування джерел електромагнітних полів з переважанням магнітної складової поля, трас прокладки прихованої (непозначеної) електропроводки, потенційно придатної для установки ЗП. До таких закладних пристроїв відносяться:

- вихідні трансформатори підсилювачів звукової частоти;

- динамічні гучномовці акустичних систем;
- електродвигуни диктофонів і магнітофонів.

Особливості режиму детектора низькочастотних магнітних полів.

У цьому режимі прилад забезпечує прийом на зовнішню магнітну антену і відображення параметрів сигналів від джерел низькочастотних електромагнітних полів з переважаючою, (наявною) магнітною складовою поля в діапазоні від 300 до 5000Гц.

Ідентифікація сигналів і їх джерел здійснюється на основі аналізу автоматично виведеної на екран дисплея осцилограми, що відображає форму прийнятого сигналу і поточне значення його амплітуди. Підвищення достовірності ідентифікації сигналів і їх джерел забезпечується можливістю одночасного з аналізом зображення на екрані дисплея, прослуховування «фонові» обстановки з використанням вбудованого гучномовця або головних телефонів.

Для роботи в умовах складної заводної обстановки передбачено диференційний режим антени, що вводиться в дію перемикачем на її корпусі.

Підготовка приладу.

Підключити зовнішню магнітну антену до сполучного кабелю, а сам кабель - до роз'єму «PROBES». Включити живлення приладу. Осцилографічний контроль параметрів прийнятого по магнітному полю сигналу включається автоматично.

Візуально по амплітуді і характером сигналу на осцилограмі і «на слух» по його тональності у вбудованому гучномовці або навушниках оцінити рівень магнітного поля і присутність фону електромережі 220В, 50Гц або її гармонік. При необхідності (в разі високого рівня фону електромережі) включити диференційний режим антени перемикачем на її корпусі (положення «до білої точки»).

Пошук сигналів і локалізація джерел.

Для низькочастотних магнітних каналів передачі інформації характерно те, що вони виникають при використанні за цільовим призначенням санкціонованих засобів (ПЕОМ, переговорних пристроїв, систем звукопідсилення, магнітофонів, телефонів і т.д.). Тому одним з основних завдань слід вважати дослідження таких засобів на наявність, інтенсивність і дальність низькочастотного магнітного поля. Супутніми можуть вважатися завдання пошуку прихованої (несанкціоновано прокладеної) проводки і виявлення працюючих диктофонів.

Потенційні джерела небезпечних низькочастотних магнітних полів слід перевіряти окремо, включаючи їх в роботу по черзі.

При дослідженні технічних засобів необхідно оцінити дальність поширення магнітних полів і особливості їх спектра. Для цього спочатку розмістити магнітну антену в безпосередній близькості до досліджуваного об'єкта. Зафіксувати по осцилограмі відносний рівень поля. Віддаляючись від досліджуваного засобу і змінюючи просторову орієнтацію антени, оцінити дальність впевненого прийому низькочастотного сигналу.

При пошуку підсилювачів звукової частоти, що мають вихідний трансформатор, слід оцінити дальність впевненого (розбірливого) прийому мовного (тестового) сигналу. Така оцінка може послужити основою для правильного вибору місць установки відповідних засобів по відношенню до зовнішньої сторони приміщення і варіанти їх спільного розташування в приміщенні. При необхідності включити режим «SA», проаналізувати спектрограму і записати її в незалежну пам'ять.

Для пошуку прихованої проводки необхідно послідовно обійти всі стіни приміщення, маючи в своєму розпорядженні магнітну антену в безпосередній близькості до них. Зафіксувати область зростання рівня поля і шляхом переміщення антени по горизонталі і вертикалі визначити проходження траси прихованої проводки.

Можливість виявлення працюючих диктофонів визначається як рівнем магнітного поля, що створюється їх двигунами, так і рівнем магнітного фону приміщення. Виявлення таких засобів можливе на відстані не більше 30 см.

Результати роботи інструментального контролю приладом ST 031 в даному режимі заносяться в облікову і звітну документацію (дод. 6).

6.4. Пошук закладних пристроїв, що використовують інфрачервоне випромінювання.

Для пошуку ЗП, що використовують інфрачервоне випромінювання, застосовується багатофункціональний пошуковий прилад SWT 031 «Піранья» в режимі детектора інфрачервоних випромінювань (INFRARED CHANNEL).

Цей режим призначений для пошуку пристроїв несанкціонованої передачі інформації в інфрачервоному діапазоні частот. До таких закладних пристроїв відносяться:

- ЗП добування акустичної інформації з її подальшою передачею в ІЧ діапазоні;
- технічні засоби просторового стеження в ІЧ-діапазоні;
- лазерні системи знімання акустичної інформації.

Підготовка до роботи.

Підключіть ІЧ датчик до гнізда «PROBES».

Увімкніть прилад. На дисплеї приладу повинен короткочасно з'явитися напис "INFRARED CHANNEL".

Перевірте працездатність приладу в даному режимі. В якості тестового датчика інфрачервоного випромінювання можна використовувати будь-який ІК пульт дистанційного керування від побутової аудіо- та відеоапаратури.

При установці порога не спрямовуйте ІЧ датчик в сторону потужних джерел ІК випромінювань (електронагрівальні прилади, лампи розжарювання, прямі сонячні промені).

Пошук сигналів і локалізація джерел.

Особливості ІЧ передавачів:

а) необхідний прямий оптично прозорий канал між ІЧ передавачем і прийомним пристроєм;

б) можлива наявність вузької діаграми спрямованості ГЧ передавача.

З урахуванням наведених особливостей, пошук небезпечних сигналів слід починати від вікон приміщення, переміщаючись в глиб приміщення, і змінюючи при цьому просторову орієнтацію ГЧ датчика.

Аналіз виявлених сигналів проводиться "на слух" в режимі "AUD", а також візуально, використовуючи режими "OSC", "SA". Локалізація таких пристроїв може здійснюватися як амплітудним методом, так і методом акустозав'язки.

Результати роботи інструментального контролю приладом ST 031 в даному режимі заносяться в облікову і звітну документацію (дод. 6).

6.5. Пошук пасивних закладних пристроїв.

Для пошуку пасивних ЗП (що знаходяться в вимкненому стані), а також ЗП з низьким рівнем демаскуючих ознак, застосовується нелінійний локатор NR 900 EM .

Принцип дії даного приладу заснований на методі нелінійної локації. Суть його полягає в тому, що всі нелінійні компоненти радіоелектронних пристроїв (напівпровідникові прилади) мають фізичну властивість випромінювати в ефір, при опроміненні їх НВЧ сигналами, гармонійні складові, кратні частоті опромінення. Таким чином можна виявити будь-які закладні пристрої, що мають в своєму складі напівпровідники. До таких закладних пристроїв відносяться:

- пасивні ЗП;
- ЗП з прихованими каналами передачі;
- ЗП з низьким рівнем ДМП;
- ЗП ультразвукового і інфрачервоного діапазонів;
- засоби звукозапису: диктофони, магнітофони.

Особливості роботи нелінійного локатора.

Нелінійний локатор має в своєму складі один передавач і два приймача, налаштованих на 2-гу і 3-ю гармоніки. Після включення NR 900 EM відбувається опромінення підстильної поверхні НВЧ сигналом. Напівпровідниковими приладами, що знаходяться в зоні опромінення, сигнал перевипромінюється і приймається приймальними антенами. Приймачі дозволяють представляти оператору рівень гармонійних складових відбитого сигналу в візуальній та звуковій формі. Визначення нелінійних компонентів можливо на відстані близько 0,7 м від передавальної антени. Енергетичний потенціал локатора забезпечує ефективний пошук впроваджених ЗП в елементи інтер'єру і в огорожувальні будівельні конструкції. Однак, суттєвим недоліком локатора є складність ідентифікації штучних напівпровідників від природних (корозійних) нелінійних відбивачів. Крім того за допомогою нелінійного локатора не виявляються:

- ЗП, розташовані в порожнинах металевих предметів;
- ЗП, розташовані в конструктивно складних електротехнічних виробках (холодильник, кондиціонер і ін.);

- ЗП, розташовані в радіотехнічних та електронних пристроях загального призначення;
- ЗП, які не мають напівпровідникових приладів, працюють в мікрохвильовому діапазоні частот, мають високу ступінь екранування.

Незважаючи на перераховані недоліки, даний локаатор є найбільш ефективним засобом для виявлення і пошуку пасивних ЗП.

У додатку 4 наведено докладний опис нелінійного локаатора і порядок роботи з ним.

Підготовка локаатора до роботи.

Закріпити антенну систему на штанзі за допомогою вузла кріплення. Підключити антенну систему до прийомопередавача, дотримуючись кольорового маркування. Включення локаатора без підключеної антеної системи не допускається.

Підключити навушники до гнізда «PHONE» приймача. Встановити акумулятор або підключити роз'єм адаптера електроживлення до гнізда DC 15 V. Підключити кабель пульта управління до гнізда CONTROL приймача. На екрані РКІ повинен відобразитися напис: "RADAR TURNED OFF". Пристрій готовий до включення.

Порядок виявлення та пошуку закладних пристроїв.

Перед включенням пристрою переконатися в підключенні антенної системи.

Лише один раз натиснути кнопку ON / OFF пульта управління - повинен включитися режим, при якому передавач установлений, приймачі включені, атенюатори приймачів встановлені в положення мінус 10 дБ, навушники підключені до виходу приймача другої гармоніки, гучність - в середньому положенні.

За допомогою кнопки АТТ встановити максимальну чутливість приймачів, на екрані РКІ в лівій частині 1-го і 2-го рядка повинні відтворюватись символи 00. Спрямовуючи антенну систему в різні боки і підключаючи кнопкою OUT 2/3 навушники до виходів приймачів другої і третьої гармонік, переконатися у відсутності перешкод на частотах прийому при максимальній чутливості приймачів. В іншому випадку оцінити можливість роботи з локаатором, встановивши атенюатори приймачів таким чином, щоб сигнал перешкоди виявився нижче порога чутливості.

Вдруге натиснути кнопку ON / OFF пульта управління - повинен включитися режим «300» - вихідна потужність передавача максимальна.

Примітка. Третє натискання кнопки ON / OFF - вимкнення пристрою, при цьому на РКІ з'являється напис: "RADAR TURNED OFF".

Перемикання навушників з однієї гармоніки на іншу здійснюється кнопкою OUT 2/3. У разі перевантаження приймачів в цьому рядку проявляється напис: "OVER".

Зміна потужності здійснюється кнопкою MAX / MIN.

За допомогою штатного імітатора переконатися в працездатності пристрою. Для цього розташувати імітатор у вільному місці при відсутності поблизу радіоелектронної апаратури. Встановити

максимальний рівень зонduючого сигналу за допомогою кнопки MAX / MIN і максимальну чутливість за допомогою кнопки ATT. За допомогою кнопки OUT 2/3 переключити навушники на вихід приймача 2-ої гармоніки. Направити антенну систему в бік імітатора з відстані 0,7-0,8 м. В навушниках повинен прослуховуватися тональний сигнал частотою 300 Гц середньої гучності, а на екрані РКІ в 1-му і 2-му рядку повинен відтворюватись рівень прийнятого сигналу 2-ої і 3-ої гармоніки відповідно. Причому рівень, на дисплеї в правій частині, повинен бути не менше 10-15 і 5-10 дБ відповідно, а різниця рівнів, яку вказують в 3-му рядку, повинна бути не менше 5 дБ. Відалення імітатора із зони зондування при незмінному положенні антеної системи повинно приводити до зникнення сигналу-відгуку.

Провести пошук напівпровідникових елементів, працюючи в залежності від завадної обстановки по можливості з максимальною потужністю і максимально можливою чутливістю. Для цього переміщати антенну систему уздовж обстежуваної поверхні. При появі в навушниках тонального сигналу частотою 300 Гц грубо визначити місце розташування перевідбиваючого об'єкта. У міру наближення до нього антеної системи інтенсивність тону в навушниках буде посилюватися.

Стежити за співвідношенням сигналів-відгуків 2-ої і 3-ої гармонік на екрані РКІ. У разі істотного перевищення рівня сигналу 3-ої гармоніки над 2-ою, найбільш ймовірно, що джерелом сигналу-відгуку є корозійна нелінійність.

Для більш достовірної ідентифікації відгуку, що не змінюючи орієнтацію і місце розташування антеної системи, перевести аналізатор в режим «20К». Для цього натиснути кнопку "300/20 K".

Встановити максимальну потужність передавача, максимальну чутливість приймачів і максимальну гучність сигналу в навушниках. Переконатися в тому, що прослуховуються модуляційні сигнали другої гармоніки зонduючого сигналу.

Максимально наблизити антенну систему до поверхні що обстежується в точці виявлення перевідбиваючого об'єкта. Переміщати антену паралельно обстежуваній поверхні від точки виявлення до периферії на 30 ... 40 см і назад, стежити за рівнем шумового сигналу в навушниках.

Залежно від характеру перевідбиваючого об'єкта - корозійний діод або штучний напівпровідний елемент (радіоелектронний пристрій), можливо дві принципово різних залежності рівня шуму в навушниках від переміщення антеної системи уздовж обстежуваної поверхні. Їх типовий вигляд представлений на рис. 5, 6.

Для підвищення достовірності рекомендується прослуховувати шумовий відгук в навушниках аналізатора в режимі «20К» при простукуванні місця розташування відбиваючого об'єкта, будь-яким неметалевим предметом. При цьому корозійний діод, як правило, характеризується хрипким нерегулярним хрустом.

При переході в режим прослуховування модуляції третьої гармоніки зонduючого сигналу, залежно від шумів в навушниках, протилежні (криві, зображені на рис. 5 і 6, міняються місцями).

Значне перевищення 2-ої гармоніки зонduючого сигналу над 3-ю гармонікою (20 дБ і більше) з високим ступенем ймовірності свідчить про штучний характер перевідбиття р - n -переходу.

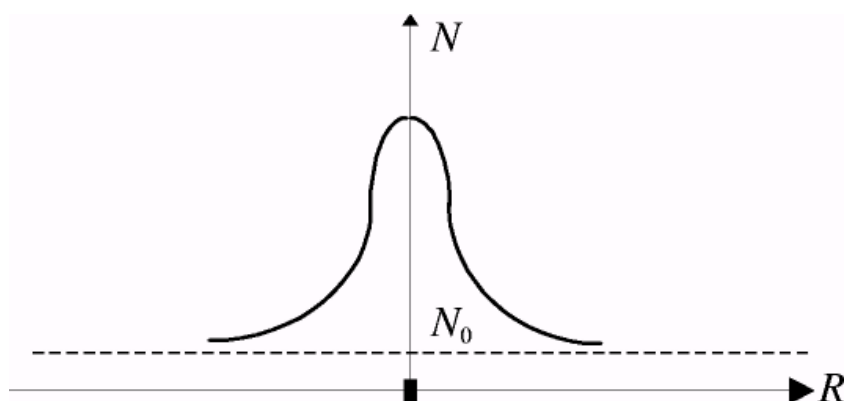


Рис. 5. Залежність рівня модуляційних шумів 2-ої гармоніки корозійного р-n-переходу від відстані від об'єкта до осі антенною системи локатора: K - точка розташування корозійного р-n - переходу; N - рівень шуму в навушниках; N_0 - рівень шуму в навушниках за відсутності нелінійного перевідбиваючого об'єкта; R - відстань від точки розташування перевідбиваючого об'єкта до осі антенної системи пристрою.

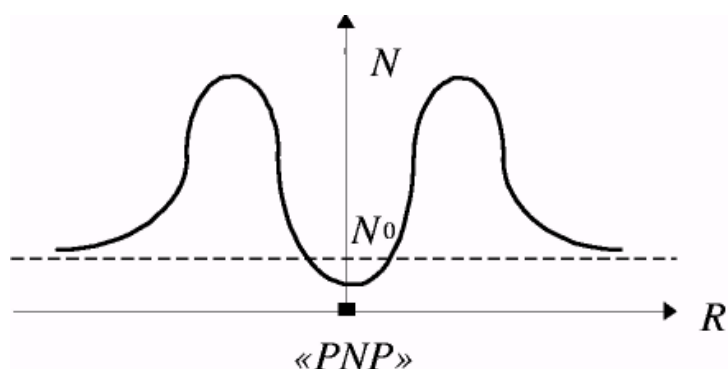


Рис. 6. Залежність рівня модуляційних шумів 2-ої гармоніки напівпровідникового р-n-переходу від відстані від об'єкта до осі антенної системи локатора: «PNP» - точка розташування напівпровідникового елемента; N - рівень шуму в навушниках; N_0 - рівень шуму в навушниках при відсутності нелінійного перевідбиваючого об'єкта; R - відстань від точки розташування перевідбиваючого об'єкта до осі антенної системи пристрою.

Результати роботи інструментального контролю приладом NR 900 ЕМ заносяться в облікову і звітну документацію (дод. 6).

6.6. Дослідження приміщень на предмет наявності акустичного і віброакустичного каналу витоку інформації.

Несанкціоноване знімання інформації акустичного характеру з обстежуваних приміщень може проводитися не тільки за допомогою закладних пристроїв, але і з інших технічних каналах витоку інформації (ТКВІ) з суміжних приміщень. До таких каналів відносяться:

- звуконепроникні будівельні огорожувальні конструкції приміщення (стіни, підлоги, стелі, вікна, двері та ін.);
- звукопровідні будівельні конструкції і системи інженерно-технічних комунікацій (опалення, водопровід і ін.);
- звуконепроникні порожнини і канали в будівельних конструкціях (повітроводи вентиляції, кабельні шахти, ніші, наскрізні отвори і ін.).

Для виявлення найбільш уразливих місць, з точки зору виникнення віброакустичних і акустичних каналів витоку інформації, а також для оцінки ефективності систем віброакустичного захисту приміщень та їх звукоізоляції застосовується пошуковий прилад ST 031 «Піранья» в режимах: віброакустичного приймача (VIBRO - ACOUSTIC CHANNEL) і акустичного приймача (ACOUSTIC CHANNEL).

Особливості режиму віброакустичного приймача.

У цьому режимі прилад забезпечує прийом від зовнішнього віброакустичного датчика і відображення параметрів низькочастотних сигналів в діапазоні від 300 до 6000 Гц.

Стан віброакустичного захисту приміщень оцінюється як кількісно, так і якісно.

Кількісна оцінка стану захищеності здійснюється на основі аналізу осцилограми, яка автоматично виводиться на екран дисплея, що відображає форму прийнятого сигналу і поточне значення його амплітуди.

Якісна оцінка стану захищеності заснована на безпосередньому прослуховуванні прийнятого низькочастотного сигналу і аналізі його гучності і тембрових характеристик. Для цього використовується або вбудований гучномовець, або навушники.

Особливості режиму акустичного приймача.

У цьому режимі прилад забезпечує прийом на зовнішній виносний мікрофон і відображення параметрів акустичних сигналів в діапазоні від 300 до 6000 Гц.

Стан звукоізоляції приміщень і наявність в них вразливих, з точки зору витоку інформації, місць визначається як кількісно, так і якісно.

Кількісно оцінка стану звукоізоляції приміщень і виявлення можливих каналів витоку інформації здійснюється на основі аналізу осцилограми, яка автоматично виводиться на екран дисплея, що відбиває форму прийнятого сигналу і поточне значення його амплітуди.

Якісна оцінка заснована на безпосередньому прослуховуванні прийнятого акустичного сигналу та аналізі його гучності і тембрових

характеристик. Для цього використовується або вбудований гучномовець, або навушники.

Підготовка приладу.

Для включення приладу в режим віброакустичного приймача необхідно підключити зовнішній віброакустичний датчик до гнізда «PROBES». Включити живлення приладу. Осцилографічний контроль параметрів прийнятого по віброакустичному каналу сигналу включається автоматично.

Для включення приладу в режим акустичного приймача необхідно підключити виносний мікрофон до гнізда «PROBES». Включити живлення приладу. Осцилографічний контроль параметрів прийнятого акустичного сигналу включається автоматично.

Оцінка ефективності віброакустичного захисту і звукоізоляції приміщень.

Об'єднання цих напрямків використання приладу визначається спільністю джерел виникнення каналів витоку інформації (мовний сигнал в акустичному діапазоні), подібністю прийомів контролю і практичною ідентичністю задіяння можливостей ST 031 «Піранья».

По-перше, і в тому, і в іншому випадку при підготовці приміщення необхідно вимкнути прилади та засоби, що створюють додатковий акустичний фон.

По-друге, в обох випадках слід використовувати тестові, а найкраще калібровані, джерела звукового сигналу.

По-третє, в суміжних, по відношенню до приміщень, які перевіряються повинен бути забезпечений мінімально можливий рівень акустичного фону.

По-четверте, застосовують практично однакові методи аналізу сигналів («на слух», по осцилограмах і спектрограмах).

Оцінка ефективності віброакустичного захисту приміщення зазвичай проводиться в два етапи. На першому етапі захист, якщо він є, повинен бути виключений і проведена перевірка власне віброакустичних властивостей огорожувальних приміщень поверхонь. Для цього необхідно віброакустичний датчик прикріплювати в різних місцях поверхонь, які перевіряються (стін, дверей, вікон, по можливості підлоги і стелі) з зовнішньої, по відношенню до контрольованого приміщення, сторони.

Включити джерело тестового звукового сигналу. Він може розміщуватися або в звичайному місці ведення конфіденційних розмов, або на певній відстані від обстежуваної поверхні (наприклад, як показано на рис. 7).

Рівень звуку зазвичай встановлюють відповідним гучному мовленню (74Дб). Для каліброваних джерел звуку відстань «L» вибирають в межах 1-2 м. Спочатку на якісному рівні (шляхом прямого прослуховування) оцінюються віброакустичні властивості обстежуваних поверхонь, а потім, переходом в режим «SA», кількісно оцінюються амплітуди частотних складових тестового сигналу.

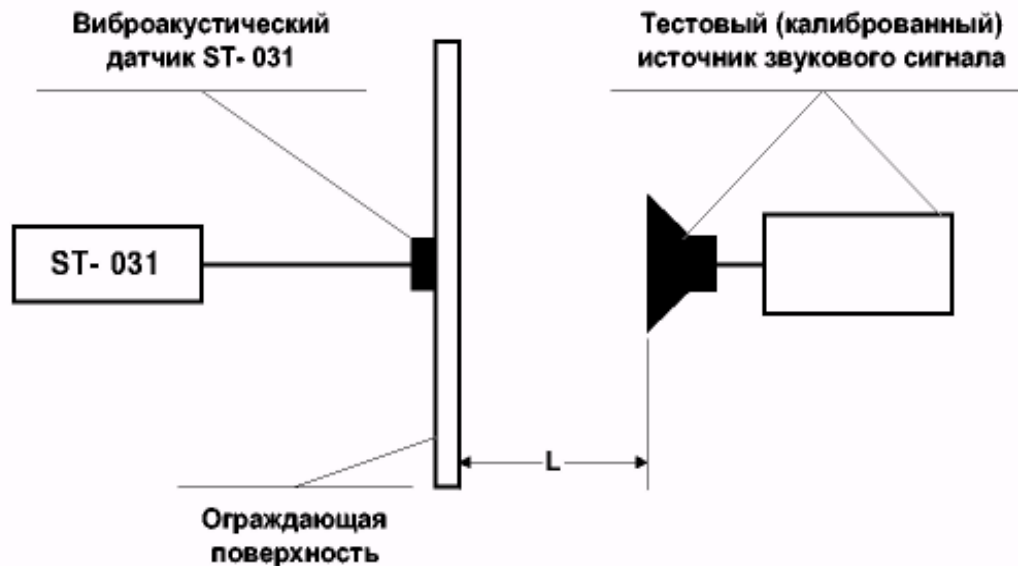


Рис. 7. Схема оцінки віброакустичних властивостей і віброакустичного захисту приміщень

На другому етапі, якщо це передбачено, оцінюється ефективність системи віброакустичного захисту. Для цього на кожній поверхні як якісно «на слух», так і кількісно по спектрограмі визначається співвідношення рівнів тестового і маскувального сигналу, а також виявляються «неприховані» складові спектра. Це служить об'єктивною основою корекції амплітудно-частотної характеристики джерел маскувального сигналу.

Відповідно до загальноприйнятих правил розбірливість мовних сигналів гарантовано не відновлюється, якщо шум, який маскує (перешкода) в 4-5 разів (16дБ) перевищує їх рівень. Повне виключення ознак мови досягається при 8-ми кратному перевищенні рівня сигналу перешкодою, створюваною системою активного захисту.

Оцінку звукоізоляції приміщень також доцільно проводити в два етапи.

На першому етапі, використовуючи тестове джерело сигналу з рівнем звуку, відповідним гучному мовленню, встановити відповідність між цим рівнем і показаннями приладу ST 031 в режимах осцилографа і аналізатора спектра. Для цього розмістити акустичний випромінювач джерела звуку і мікрофон приладу ST 031 на деякій фіксованій відстані. Зазвичай її вибирають в межах 1-2 м (рис. 8).

На другому етапі оцінюються звукоізоляційні властивості огорожувальних поверхонь приміщення (стін, дверей, вікон, а якщо можливо, то підлоги і стелі), ефективність системи активного захисту (зашумлення), а також можливість витоку мовної акустичної інформації через елементи вентиляції, різного роду ніші, наскрізні отвори і т.п.

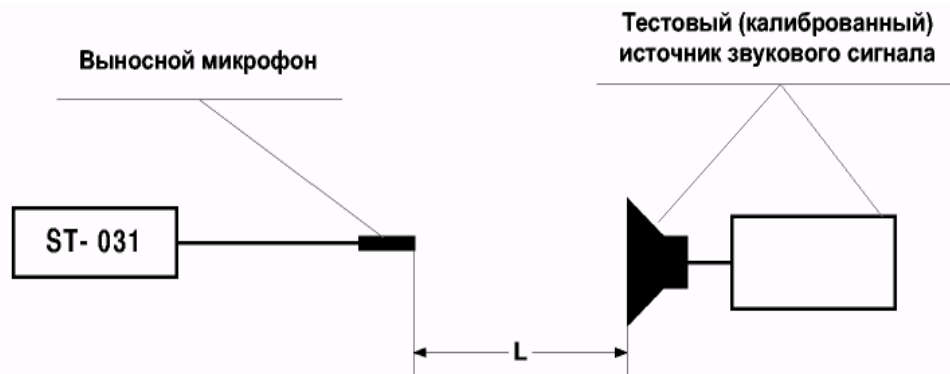


Рис.8. Схема калібрування індикаторів рівня звукового сигналу прилада ST 031

Для оцінки звукоізоляційних властивостей стін, дверей (підлоги, стелі) тестове джерело звуку може бути розташованим або в звичайному місці ведення конфіденційних розмов, або на відстані від обстежуваної поверхні. Наприклад, у варіанті показаному на рис. 9.

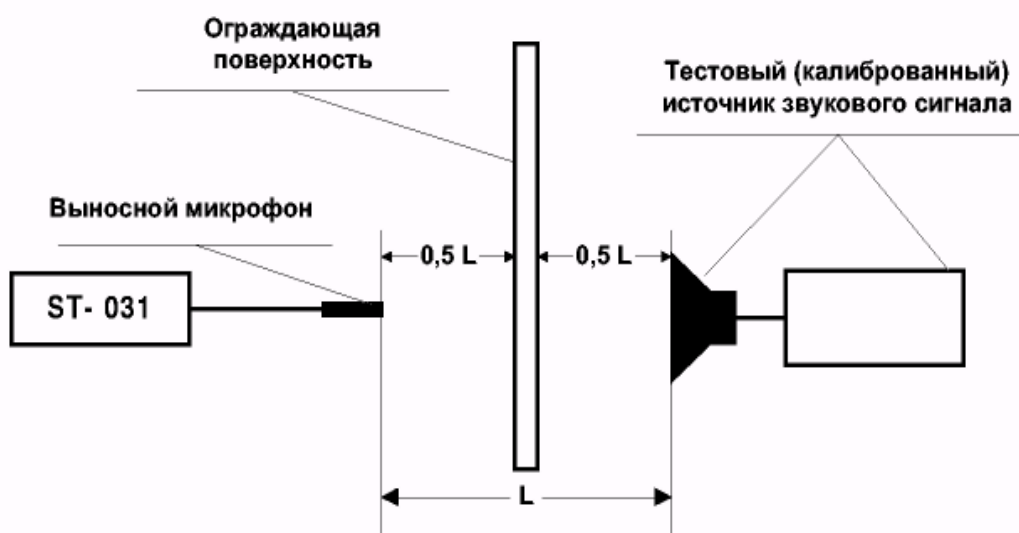


Рис. 9. Схема оцінки звукоізоляції приміщень

Розміщуючи мікрофон в різних місцях суміжних (вище і нижче розташованих) приміщень якісно «на слух» і кількісно по спектрограмі визначити дальність перехоплення мовної інформації з даного приміщення і оцінити зниження рівня звукового сигналу за рахунок властивостей огорожувальних поверхонь, а також наявність найменш ослаблених складових спектра. Останнє дає можливість прийняти обґрунтоване рішення про необхідність додаткового захисту, в тому числі активного і вибір характеристик засобів захисту.

Якщо приміщення розташоване вище першого поверху, виникають певні труднощі в перевірці звукоізоляції віконних конструкцій. В цьому випадку достатній для якісної оцінки ефект дає наступний, часто використовуваний прийом. Тестове джерело звуку розміщується за

допомогою одного з раніше розглянутих варіантів. Відкривається кватирка, фрамуга або інша частина вікна, в залежності від особливостей віконних рам. Мікрофон вивішується назовні і в цьому положенні фіксується рівень прийнятого ним тестового сигналу з приміщення. Потім відкрита частина вікна обережно (щоб не пошкодити кабель мікрофона), але, по можливості, щільно прикривається. Якісно «на слух» і кількісно по осцилограмі або спектрограмі оцінюються звукоізоляційні властивості віконних конструкцій.

Оскільки повітроводи систем вентиляції прийнято розглядати як найбільш небезпечні канали витоку мовної акустичної інформації, то вони підлягають обов'язковій перевірці. Для цього мікрофон приладу ST 031 необхідно ввести в вихідний (вхідний) отвір повітропроводу кожного з суміжних приміщень, а можливо і деяких інших. Якісно «на слух» оцінити проходження і розбірливість сигналу від тестового джерела, а за показниками приладу ST 031 в режимі осцилографа або аналізатора спектра його ослаблення при проходженні по повітропроводу до місця розміщення мікрофона. При цьому правильна оцінка ослаблення може бути отримана тільки в тому випадку, якщо є детальна схема системи вентиляції. Її наявність дає можливість врахувати ослаблення, що вноситься різними елементами конструкції повітропроводів. Так, ослаблення мовного сигналу зазвичай становить:

0,15 дБ/м - в прямих металевих повітропроводах;

0,2 - 0,3 дБ/м - в прямих не металевих повітропроводах;

1,0 - 3,0 дБ/м - при зміні перетину повітропроводу;

3,0 - 7,0 дБ/м - на один вигин повітропроводу.

Результати перевірки служать об'єктивною основою для рішення про необхідність додаткового захисту, для вибору заходів та засобів його забезпечення. Всі результати роботи за даними перевірок заносяться в облікову і звітну документацію (дод. 6).

6.7. Візуальний огляд і фізичний пошук закладних пристроїв.

За результатами інструментального контролю, локалізації місця розташування закладних пристроїв здійснюється фізичний пошук і знешкодження ЗП. Візуальний огляд огорожувальних конструкцій, меблів та інших предметів інтер'єру приміщень на наявність в них закладних пристроїв є обов'язковим і необхідним елементом пошукових робіт. Ретельний огляд завжди пов'язаний з переміщенням меблів і предметів, які після закінчення перевірки приміщення повинні бути залишені в тому положенні і вигляді, в якому вони перебували до початку огляду. Тому перед початком огляду проводиться протоколювання, аж до фотографування, розміщення всіх предметів, що знаходяться в приміщенні.

В процесі огляду слід шукати нові, раніше не властиві даному приміщенню, можливо підкинуті предмети, а також ознаки можливого використання елементів інтер'єру та конструкції приміщення для впровадження в них закладних пристроїв. До таких ознак належать:

- перестановка меблів і предметів, поява на них нових, що раніше не відзначалися елементів і деталей;
- зміщення предметів, покриттів і меблів з їх звичайних місць;
- сліди розтину панелей і інших знімних елементів конструкції приміщення і предметів;
- сліди недавньої закладення отворів, свіжої штукатурки або фарбування поверхонь і т. п.

При візуальному огляді приміщення рекомендується:

- підняти і оглянути знизу покриття для підлоги (килими, паласи, лінолеум), звертаючи увагу на нехарактерні для даного покриття ділянки: вставки, підклеювання, латки;
- оглянути поверхню підлоги, досліджувати місця зі слідами недавнього фарбування, ремонту, застосування інструменту, що порушує цілісність поверхні;
- оглянути плінтуси, ретельно досліджувати місця зі слідами недавнього ремонту і можливого вторгнення, в необхідних випадках провести їх тимчасовий демонтаж для огляду простору під плінтусами, переконатися у відсутності під плінтусами струмопровідникових і оптоволоконних ліній;
- розкрити і оглянути канали під підлогою, звертаючи особливу увагу на нижню сторону знімних кришок, наявні пази і щілини, сліди їх нещодавньої закладення; ретельно, на максимально можливу глибину із застосуванням ендоскопа оглянути вміст труб, що підходять до підпідлогових каналів, переконатися у відсутності в них сторонніх предметів і проводів; штатні дроти та кабелі в ході огляду рекомендується витягнути з закладних труб (кабельних каналів) на максимально можливу довжину для того, щоб переконатися у відсутності несанкціонованих підключень до проводів;
- ретельно оглянути місця наскрізного проходження крізь підлогу водопровідних труб, труб парового опалення і інших комунікацій, оскільки в цих місцях найпростіше замаскувати сліди вторгнення при установці засобів НДІ.

Візуальний огляд стін. При огляді стін необхідно:

- звільнити їх поверхню від накладених предметів і покриттів (картин, дзеркал, килимів і т. п.);
- оглянути поверхню стін, звертаючи особливу увагу на місця, що відрізняються за своїм забарвленням або фактурою від решти поверхні; відзначити підозрілі місця на плані приміщення для подальшого їх дослідження за допомогою спеціальних технічних засобів;
- в разі обклеювання поверхні стін шпалерами ретельно оглянути місця нерівностей, стиків шпалер, латок, порізів і надривів, пересвідчитися в щільності прилягання шпалер до поверхні стіни; при необхідності розкрити шпалери, які відшарувалися для перевірки вмісту утвореної порожнини;
- в разі підшивань стін особливу увагу звернути на наявність слідів висвердлювання і подальшого забивання отворів;

- при наявності в стінах технологічних, комунікаційних та інших ніш, які закриваються знімними кришками або панелями, огляд ніш проводити відповідно до рекомендацій по огляду підпідлогових каналів.

При візуальному огляді вентиляційних та інших технологічних отворів і порожнин рекомендується:

- перевірити недоторканність решітки, яка закриває отвір або кришки по нанесених в ході попередньої перевірки спеціальних мітках;
- зняти ґрати, які закривають отвір, переконатися у відсутності слідів порушення пилового шару навколо отвору і на внутрішніх його поверхнях;
- переконатися у відсутності сторонніх предметів і проводів в отворі, порожнинах і трубах, які підходять до порожнини, для чого використовувати оглядові дзеркала, ендоскопи та ліхтарі.

При візуальному огляді вікон необхідно:

- провести огляд поверхонь підвіконня, віконного отвору і віконної рами, звертаючи особливу увагу на наявні щілини і порожнини, щільність прилягання і однорідність кріплення ущільнень, сліди порушення цілості поверхні;
- відкрити вікно і переконатися у відсутності сторонніх провідників і предметів на внутрішніх і зовнішніх поверхнях віконної рами, слідів демонтажу або заміни ущільнень, запірних елементів, елементів кріплення;
- в разі здвоєних рам провести їх розбирання, переконатися у відсутності сторонніх провідників і предметів в між рамними щілинами;
- уважно оглянути всі поверхні і порожнини карнизів і жалюзі, складки штор, переконатися у відсутності сторонніх предметів;
- оглядом прилеглих до віконного прорізу ділянок зовнішніх стін переконатися у відсутності на них сторонніх предметів, латок чи інших слідів можливого вторгнення; особливу увагу слід звернути на ділянки, приховані від поверхневого огляду водовідбійних козирків.

У більшості приміщень під вікнами розміщені радіатори системи парового опалення. Складна конфігурація радіаторів, часто зустрічається застосування декоративних екранів, які приховують радіатори і труби системи опалення від спостереження, створюють сприятливі умови для установки в цих місцях закладних пристроїв.

При візуальному огляді дверей рекомендується:

- оглянути щілини за лиштвами дверної коробки, переконуються у відсутності слідів демонтажу наличників; в разі підозр на їх розкриття демонтувати лиштви, оглянути приховані ними пази і щілини, переконатися у відсутності слідів їх недавнього закладення;
- переконатися у відсутності слідів розтину дверної оббивки і дверного полотна, в підозрілих випадках зняти і оглянути зворотній бік дверної оббивки і приховану оббивкою поверхню дверного полотна;

- оглянути елементи навішування дверей і переконатися у відсутності слідів їх демонтажу; в разі підозр демонтувати дверні петлі і оглянути приховану за ними поверхню дверної коробки або дверного полотна;
- при огляді металевих дверей звернути особливу увагу на сліди висвердлювання отворів в дверному полотні і дверній коробці, сліди тимчасового демонтажу запірних елементів і елементів навіски дверей; в підозрілих випадках демонтувати замок і оглянути внутрішні порожнини дверного полотна за допомогою ендоскопа.

При візуальному огляді стелі слід звернути увагу на ділянки зі слідами недавнього фарбування, ремонту, протікання, наскрізного проходження труб та інших комунікацій. Особливої уваги потребує огляд підвісної стелі. Така стеля складається зі знімних, що закріплюються на каркасі, панелей і легко може бути використана зловмисником для установки ЗП. Огляд підвісної стелі, як правило, поєднується з візуальним оглядом та перевіркою ліній і встановленого на стелі обладнання провідних комунікацій.

Перед розкриттям стельових панелей слід переконатися в цілісності міток, залишених в ході попередньої перевірки. У разі порушення міток або виявленні слідів можливого розкриття панелей огляд запанельного простору слід почати з підозрілих місць. При розтині панелей насамперед оглядається їх зворотна сторона. Особливу увагу слід приділити огляду пазів і непроглядних знизу поверхонь каркаса. Використання оглядових дзеркал при цьому абсолютно необхідно. В процесі огляду запанельного простору проводиться паралельний огляд з демонтажем і розбиранням освітлювальних, сигналізаційних та інших приладів, змонтованих на стелі.

Візуальний огляд меблів проводиться в наступній послідовності:

- поверхні меблів (полиці, ящики, сидіння і т. п.) звільняються від предметів і покриттів, виймальні і легкознімальні елементи видаляються для окремого огляду;
- оглядаються поверхні основних конструктивних елементів для виявлення закріплених сторонніх предметів і деталей, отворів неясного призначення, вставок, наклейок, швів, інших слідів вторгнення; особлива увага приділяється порівнянню товщини стінок і панелей, огляду задніх і нижніх поверхонь елементів, пазів і щілин, а також складок і швів оббивки м'яких меблів;
- оглядаються поверхні кріпильних і сполучних елементів для виявлення слідів можливого демонтажу меблів з метою приховування за сполучними елементами засобів НДІ; для полегшення подальшого контролю недоторканності кріпильних і сполучних елементів доцільно покрити головки кріпильних деталей і місця з'єднання елементів тонким шаром маркованої фарби;
- проводиться огляд зовнішніх і внутрішніх поверхонь, що виймаються і легкознімальних елементів відповідно до рекомендацій з огляду основних конструктивних елементів.

По завершенні огляду меблів, а іноді і паралельно з ним проводиться візуальний огляд інших предметів інтер'єру приміщення: які окремо стоять на

підлозі, розвішаних на стінах, розміщених на підвіконнях або поверхнях меблів.

З особливою ретельністю слід оглядати предмети, які постійно перебувають на столі або в безпосередній близькості від робочого столу керівника. Огляду і перевірці підлягають папки з документацією, книги, рами картин і дзеркал, кошики для сміття, квіткові горщики і кімнатні рослини, годинник, статуетки та інші предмети, що мають всередині себе порожнини, розміри яких дозволяють розмістити в них ЗП.

Рекомендується проводити фізичний пошук і візуальний огляд не тільки в тих приміщеннях, на які вказав керівник підприємства, який замовив перевірку, а й в суміжних з ними.

Виявлення замаскованого диктофона, підкинутого радіомікрофона або іншого засобу НДІ не повинно стати причиною поверхневого виконання інших передбачених планом пошукових робіт, тим більше, їх згортання і припинення.

Результати роботи з фізичного пошуку закладних пристроїв та візуальним оглядом приміщень заносяться в облікову і звітну документацію (дод. 6).

7. МЕТОДИКА ВИКОНАННЯ РОБІТ НА ЗАКЛЮЧНОМУ ЕТАПІ КОМПЛЕКСНОЇ СПЕЦІАЛЬНОЇ ПЕРЕВІРКИ ПРИМІЩЕНЬ

Заклучний етап перевірки є завершальним всіх пошукових заходів.

Метою заклучного етапу є обробка результатів перевірки, оформлення звітної документації, підготовка акту перевірки приміщення.

На початку заклучного етапу виконується обробка результатів перевірки, оформлення протоколів вимірювань, проведення необхідних інженерних розрахунків. Якщо на об'єкті виявлено закладний пристрій, то, за результатами вимірювання частоти і амплітуди випромінюваного електромагнітного поля, для нього розраховується максимальна дальність від ЗП до можливих засобів реєстрації інформації.

Для вивчення нових, невідомих раніше засобів НДІ визначаються технічні характеристики і споживчі властивості виявлених закладних пристроїв, визначається орієнтовний час та спосіб їх закладки. На основі вивчення цих даних детально аналізуються демаскуючі ознаки виявлених ЗП і проводиться їх ідентифікація відповідно до класифікації ЗП (розділ 2). При необхідності слід провести додаткові інструментальні перевірки для виявлених демаскуючих ознак і методів їх маскуваня.

Для складання акта перевірки виконується опис проведених робіт і досліджень з додатком використовуваних схем і планів приміщень.

На основі результатів інструментального контролю і фізичного пошуку розробляються рекомендації з підвищення захищеності приміщень, що перевіряються. Для складання рекомендацій виконуються наступні роботи:

- складається перелік і схеми виявлених ТКВІ;

- проводиться оцінка ступеня існуючого захисту кожного приміщення, яке перевіряється від засобів НДІ за виявленими ТКВІ;
- розробляються додаткові заходи та способи захисту по кожному виявленому каналу;
- складається перелік технічних засобів і систем, рекомендованих до установки для захисту інформації від витоку технічними каналами;
- розробляються пропозиції щодо способів використання рекомендованих технічних засобів і систем.

На підставі проведених робіт складається акт перевірки приміщення, що включає в себе результати виконаних робіт і рекомендації (дод. 6, 7). У разі необхідності також видаються рекомендації Замовнику з перевірки комп'ютерів і сканерів на предмет наявності в них впроваджених ЗП в організаціях, що надають даний вид послуг.

ВИСНОВОК

Точне виконання всіх операцій, описаних у цій Методиці, в поєднанні з високим професіоналізмом виконавців та застосуванням передового пошукового обладнання, дозволяє ефективно проводити комплексні спеціальні перевірки на наявність закладних пристроїв та інших засобів негласного знімання інформації на об'єктах підприємницької діяльності.

Ця Методика являє собою комплекс логічно взаємопов'язаних процедур і операцій, що дозволяють з високою достовірністю здійснювати виявлення, локалізацію і ідентифікацію активних закладних пристроїв за наступними демаскуючими ознаками:

- електромагнітними полями радіочастотного каналу передачі;*
- сигналами акусто-електричного перетворення в провідних комунікаціях;*
- електромагнітним випромінюванням низької частоти з переважанням магнітної складової;*
- інфрачервоному випромінюванню, яке модулюється мовними сигналами.*

Пошук пасивних закладних пристроїв, що не проявляють себе якими-небудь демаскуючими ознаками, запропоновано здійснювати новим передовим методом нелінійної локації, заснованим на фізичних властивостях всіх нелінійних компонентів радіоелектронних пристроїв випромінювати в ефір, при опроміненні НВЧ сигналами, гармонійні складові, кратні частоті опромінення.

Особливу увагу в наведеній Методиці приділяється не тільки пошуку впроваджених закладних пристроїв, а й підготовці облікової та звітної документації, виробленню рекомендацій щодо підвищення технічної захищеності інформації на об'єктах підприємницької діяльності.

Список використаних джерел

1. Закон України "Про інформацію" від 2.10.1992 р. № 2657-ХІІ.
2. Закон України "Про захист інформації а автоматизованого системах" від 5.07.1994 р. № 80/94-ВР.
3. Закон України "Про державну таємницю" від 21.01.1994 р. № 3855-ХІІ.
4. Закон України "Про ліцензування питань комерційної торгівлі відів господарської діяльності" від 1.06.2000 р. № 1775-ІІІ.
5. Положення про технічний захист інформації в Україні, затверджених постановою КМ України від 27.9.1999р. № 1229.
6. Положення про Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, затверджене постановою Кабінету Міністрів Указом Президента України від 6.10.2000 р. №1120.
7. Ліцензійні умови провадження господарської діяльності, пов'язаної з розроблення, виробництвом, Впровадження, обслуговування, Досліджень ефективності систем и засобів ТЗІ, Надання послуг у Галузі ТЗІ.
8. Рекомендації з проведення Перевірки приміщень, технічних засобів спеціального и загально призначення на наявність закладних пристроїв, призначення для знімання інформації с граничено доступом по акустичних та других каналах. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.
9. Технічні описи та Інструкції засобів технічного захисту інформації.
10. Laptev A.A., Savchenko V.A., Barabash O.V. Savchenko V.V., Matsko A.I. The metod of searching for digital vtfns of illegal obtaning of information on the basis cluster analysis. Magyar Tudományos Journal. Budapest, Hungary, 2019. № 31. P. 33 – 37
11. Laptev A., Kliukovskyi D., Barabash A., Zidan A., Analysis of Existing Signal Detection Methods, Development of a Technique for Calculating the Probability of Secret Information Capture. International Journal of Science and Engineering Investigations (IJSEI). Denmark. 2019. Vol. 8, Issue 92. P. 99 – 103.
12. Laptev A., Sobchuk V., Barabash O., Musienko A. Analysis of the main Approaches and Stages for Providing the Properties of the Functional Stability of the Information Systems of the Enterprise. Sciences of Europe. Praha, Czech Republic. 2019. Vol. 1. No 42. P. 41 – 44.
13. Лаптев О.А., Войченко Т.О., Кудюкін П.В., Степаненко В.І. Метод оцінки параметрів сигналу засобів несанкціонованого знімання інформації на основі кореляційно-регресійного аналізу. Науковий журнал «Наукоемні технології» К.: НАУ, 2019. № 3 (43). С. 313 – 320.
14. Лаптев О.А., Половінкін І.М, Клюковський Д.В., Барабаш А.О. Модель пошуку засобів негласного отримання інформації на основі диференціальних перетворень. Sciences of Europe. Praha, Czech Republic, 2019. Vol. 1. No 43. ISSN 3162-2364. P. 59 – 62

15. Лаптев О.А., Собчук В.В., Савченко В.А. Метод підвищення завадостійкості системи виявлення, розпізнавання і локалізації цифрових сигналів в інформаційних системах. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2019. Вип. 66. С. 124 – 132.
16. Лаптев О.А. Методика визначення ймовірності негласного отримання інформації потенційним порушником. Science and Education a New Dimension. Natural and Technical Sciences. Budapest, Hungary, VII(24), Issue: 200, 2019. ISSN 2308-5258. P. 27 – 31.
17. Хорошко В.А., Чекатков А.А., Ковтанюк Ю.С. Методы и средства защиты информации. К.: Юниор. 2003. 502 с.
18. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. К.: 2003. 214 с.
19. Хорошко В.О. Хохлачова Ю.Є. Оцінка захищеності інформаційних систем. Сучасний захист інформації. 2012. № 4. С. 50 – 57.
20. Указ Президента України від 27 вересня 1999 року № 1229 «Положення про технічний захист інформації в Україні».
21. Силантьев В.А. Применение векторных анализаторов в системах радиоконтроля. Специальная техника. 2002. № 5. С. 25 – 37.
22. Радзиевский В.Г. Сирота А.А. Теоретические основы радиоэлектронной разведки. Закрытое акционерное общество Издательство Радиотехника. 2004. 432 с.
23. Нормативний документ системи технічного захисту інформації НД ТЗІ 1.5-001-2000 «Радіовиявлювачі. Класифікація. Загальні технічні вимоги».
24. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.3-001-2001 «Радіовиявлювачі вимірювальні. Методи та засоби випробувань».
25. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.3-004-2001 «Радіовиявлювачі індикаторні. Методи та засоби випробувань».
26. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.3-005-2001 «Радіовиявлювачі панорамні. Методи та засоби випробувань».
27. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.3-006-2001 «Радіовиявлювачі аналізувальні. Методи та засоби випробувань».
28. Нормативний документ системи технічного захисту інформації НД ТЗІ 1.4-002-08 «Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань».
29. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.7-011-2012 «Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв».

30. Обеспечение безопасности во всем мире – наша постоянная миссия [Электронный ресурс] // Symantec (Norton Security). 2015. Режим доступа: <http://www.symantec.com/ru/ru/>

31. Максименко Г.А., Хорошко В.А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств. К: ПолиграфКонсалтинг, 2004. 317 с.

32. Лаптев О.А., Дрягин А.Б., Юденко И.С., Блаженный В.И., Шевченко Ю.В. Сучасні тенденції розвитку зв'язку та радіотехнічного забезпечення польотів. Тези доповідей: Науково технічний семінар Національної академії оборони України. м.Київ, 21 січня 2003 р. С. 9 – 14.

33. Кривцун А.В. Захаров А.В. Использование новых возможностей комплекса радиомониторинга и цифрового анализа сигналов «Кассандра-М» для обнаружения современных специальных технических средств с передачей информации по радиоканалу [Электронный ресурс] режим доступа: <http://www.inspectorsoft.ru/article.php?id=388> (24.05.2019)

34. Кибершпион атакует спецслужбы Украины [Электронный ресурс] ESET. 2015. Режим доступа: <http://eset.ua/ru/news/view/390/operation-potao>.

35. Журиленко Б.Е., Хорошко В.А. Системы и устройства защиты информации. К.: НАУ, 2004. 63 с.

36. Журиленко Б.Е., Левандівська Л.І., Ніколаєва Н.К. Захист циркулюючої в приміщенні акустичної інформації тональним сигналом. Защита информации. К: НАУ, 2007. С. 36 – 39.

37. Забара С. Характеристики моделювання систем у середовищі MATLAB. К.: Вид. Университет "Украина", 2011. 137 с.

38. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України".

39. Захаров А.В. Требования к перспективному анализатору сетей

40. Wi-Fi [Электронный ресурс] Режим доступа: <http://www.analitika.info/> (25.05.2019).

41. Ананский Е.В. Что такое радиозакладки и как их обнаружить? (часть2)/журнал «Служба безопасности» [Электронный ресурс] режим доступа: <http://www.kvirin.com/articles/267/>

42. Закон України "Про інформацію".
<https://zakon.rada.gov.ua/laws/main/2657-12>

43. Закон України "Про доступ до публічної інформації".

44. Закон України "Про захист інформаційно- телекомунікаційних системах". <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>

45. За Закон України "Про основні засади забезпечення кібербезпеки України" <https://zakon.rada.gov.ua/laws/main/2163-19>

46. Закон України "Про електронні документи та електронний документообіг". <https://zakon.rada.gov.ua/laws/show/851-15>

47. Постанова Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних,

телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 № 373. <https://zakon.rada.gov.ua/laws/main/373-2006-%D0%BF>

48. Постанова Кабінету Міністрів України "Про затвердження Порядку підключення до глобальних мереж передачі даних" від 12.04.2002 р. № 522.

49. Постанова Кабінету Міністрів України "Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних" від 04.02.1998 № 121. <https://zakon.rada.gov.ua/laws/main/121-98-%D0%BF>

50. Постанова Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.2010 № 518.

51. Постанова Кабінету Міністрів України "Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію" від 19 жовтня 2016 р. № 736.

52. ДСТУ 33960-96. Захист інформації. Технічний захист інформації. Основні положення.

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?artid=38911&cat_id=38836

53. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?artid=38911&cat_id=38836

54. НД 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

<https://zakon.rada.gov.ua/rada/show/v0215519-13>

55. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&artid=302408&cat_id=89734&ctime=1547122731920

56. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=89740&cat_id=89734&ctime=1547204009788

57. НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації.

58. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі. http://www.dut.edu.ua/uploads/I_102375718671.pdf

59. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

60. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

<http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342>

61. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (зі зміною № 1).

http://dstszi.kmu.gov.ua/dstszi/control/uk/publishvarticle?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407

62. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу "2".

<http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106343>

63. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

<http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106344>

64. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв. <http://www.dsszzi.gov.ua/dsszzi/doccatalog/document%3Fid=103253>

65. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.

http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46075

66. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074

67. НД ТЗІ Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичним джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації.

http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101924&cat_id=89734&ctime=1344501363205

68. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ ПЕМВН-95).

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101798&cat_id=89734&ctime=1344500065981

69. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95).

<http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&artid=120206&catid=89769&ctime=1421836194327>

70. ДСТУ ISO/IEC 27001: 2015 Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001: 2013, IDT).

71. ДСТУ ISO/IEC 27002: 2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27003: 2013, IDT).

72. ДСТУ ISO/IEC 27005: 2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005: 2018, IDT).

73. Указ Президента України "Про Положення про технічний захист інформації в Україні" від 27.09.1999 № 1229.

74. Бурячок В.Л., Толюпа С.В., Семко В.В., Бурячок Л.В., Складанний П.М., Лукова-Чуйко Н.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Посібник. - К. : ДУТ. - КНУ, 2016. - 178 с.

75. Бурячок В.Л., Гулак Г.М., Толубко В. Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Підручник. - К.: ТОВ «СІК ГРУП УКРАЇНА», 2015. - 449 с.

76. Кобозева А.А., Мачалін І.О., Хорошко В. О. Аналіз захищеності інформаційних систем: підручник. К. ДУІКТ, 2010. - 316 с.

77. Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід / В. Гребенніков «Издательские решения», 2018. - 249 с.

78. 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.: ІСЗЗІ НТУУ "КПІ", 2016. 104 с.

79. Хорошко В.О., Азаров О.Д., Максименко Г.О., Яремчук Ю. Е. Пошук та локалізація радіозакладних пристроїв. Навчальний посібник. - Вінниця: ВНТУ, 2007. - 333 с.

80. Технічний захист інформації в інформаційних та телекомунікаційних системах: навч. посібн. / Г.І. Ластівка, П.М. Шпатар // - Чернівці, ЧНУ, 2018. 252 с.

ДОДАТКИ

ЗМІСТ

| | |
|--|-----|
| Додаток 1. Варіант плану проведення комплексної спеціальної перевірки приміщень..... | 63 |
| Додаток 2. Методика пошуку закладних пристроїв з використанням пошукового програмно-апаратного комплексу ПАК DigiScan..... | 68 |
| Додаток 3. Методика пошуку закладних пристроїв з використанням пошукового приладу ST 031 «Піранья»..... | 78 |
| Додаток 4. Методика пошуку закладних пристроїв з використанням нелінійного локатора NR-900EM..... | 103 |
| Додаток 5. Методика пошуку закладних пристроїв з використанням індикатора поля PROTECT 1203..... | 111 |
| Додаток 6. Варіант акту комплексної спеціальної перевірки приміщень..... | 115 |
| Додаток 7. Варіант рекомендацій по підвищенню захищеності перевірених приміщень і об'єктів..... | 118 |
| Додаток 8. Перелік нормативно-правових документів, на основі яких втілюється діяльність по наданню послуг з ТЗІ..... | 123 |

**ВАРІАНТ ПЛАНУ ПРОВЕДЕННЯ КОМПЛЕКСНОЇ
СПЕЦІАЛЬНОЇ ПЕРЕВІРКИ ПРИМІЩЕНЬ**

Екз.№_
Всього_екз.

Погоджено
Начальник служби
безпеки підприємства
_____/_____/_____
" ____ " _____ 20__р.

Затверджую
Керівник підприємства
_____/_____/_____
" ____ " _____ 20__р.

**ПЛАН
проведення комплексної спеціальної перевірки приміщень**

1. Висновки оцінки противника.

У якості суб'єкту, обраного вірогідним противником для встановлення закладних пристроїв (ЗП) та інших засобів несанкціонованого отримання інформації (НОІ), розглядається відвідувач (клієнт), що мав доступ до кабінету керівника підприємства та у сусідні з ним приміщення. Для встановлення засобів НОІ можливе використання противником одного з працівників, що проводив косметичний ремонт кабінету керівника у період з _ по _ (дата, час). У якості суб'єкту, що здійснював знімання інформації, був розглянутий відвідувач (клієнт) або сторонні особи за межами контрольованої зони.

Суб'єкт, що здійснював встановлення засобів НОІ, є спеціалістом по негласному зніманню інформації, володіє відомостями про розміщення необхідних йому приміщень, розміщення у них обладнання та предметів інтер'єру.

Враховуючи можливість встановлення засобів НОІ під час ремонту кабінету керівника, можна очікувати використання противником, як радіовипромінюючих ЗП, так і передаючих інформацію по дротових комунікаціях. У сусідніх приміщеннях можливе встановлення противником засобів знімання інформації з телефонних ліній та електронних стетоскопів. Очікуваний технічний і технологічний рівень застосовуваних ЗП та інших засобів НОІ відповідає середній ділянці цінового діапазону цих засобів.

Найбільш вірогідне встановлення засобів НОІ під час ремонту кабінету керівника шляхом підкидання, підключення до телефонної лінії, підміни електричних та телефонних комутаційних виробів. Можливе підкидання радіомікрофона під час відвідування кабінету відвідувачем (клієнтом). Вірогідний час встановлення засобів НОІ - у

період з _ по _ (дата, час). Очікувані способи знімання інформації – підключення до дротових ліній у сусідніх приміщеннях та перехоплення радіопередач з допомогою радіоконтрольного пункту, розміщеного за межами контрольованої території.

При виявленні противником намірів проведення спеціальної перевірки приміщень можливе тимчасове вилучення ЗП. Встановлення факту проведення такої перевірки може призвести до тимчасового вимкнення дистанційно керованих ЗП. При встановленні факту виявлення встановлених ЗП найбільш вірогідна спроба встановлення нового аналогічного пристрою.

2. Мета проведення комплексної спеціальної перевірки приміщень.

Мета проведення перевірки – запобігання збитків від витоку акустичної та відеоінформації з приміщення через потенційно встановлені ЗП.

Перевірці підлягають:

1. Кабінет керівника підприємства.

Площа приміщення – _ кв. м., об'єм – _ куб. м. Огороджувальні конструкції – залізобетонні панелі (товщина зовнішньої стінової панелі – _ см), суміжна з бухгалтерією стіна – цегляна, товщиною – _ см. Стеля підвісна, стіни штукатурені, покриті дерев'яними панелями. Два вентиляційні канали пасивної вентиляції.

Офісне обладнання: телевізор, ПЕОМ, телефонний апарат. Меблі стандартні офісні: письмовий і журнальні столи, два крісла, вбудована шафа, два стелажа, три м'які крісла, сейф, холодильник займають _ процентів загальної площі приміщення.

Дротові комунікації силової та освітлювальної електромережі, телефонна лінія, лінії пожежної і охоронної сигналізації. Магістраль парового опалення.

2. Приміщення бухгалтерії.

(наводяться характеристики другого приміщення)

Перелік запланованих робіт:

1. У кабінеті керівника підприємства:

1. Візуальних огляд огороджувальних конструкцій, меблів та інших предметів інтер'єру (очікувана трудомісткість – _ люд.годин).
2. Перевірка елементів будівних конструкцій, меблів та інших предметів інтер'єру з використанням спеціальних пошукових технічних засобів (_ люд. годин).
3. Перевірка ліній і обладнання силової та освітлювальної електромережі (_ люд. годин).
4. Перевірка ліній та обладнання абонентської телефонної мережі (_ люд. годин).

5. Перевірка ліній і обладнання пожежної та охоронної сигналізації (_ люд. годин).
 6. Перевірка радіоефіру на наявність сигналів радіовипромінюючих засобів неявного знімання інформації (радіомоніторинг приміщення) (_ люд. годин).
 7. Перевірка несанкціонованих передач інформації у діапазоні інфрачервоного випромінювання (_ люд. годин).
 8. Пошук закладних пристроїв, що використовують низькочастотні магнітні випромінювання (_ люд. годин).
 9. Пошук пасивних закладних пристроїв (_ люд. годин).
 10. Дослідження приміщення на предмет наявності приладів та інших засобів НОІ (_ люд. годин).
 11. Фізичний пошук закладних пристроїв та інших засобів НОІ (_ люд. годин).
2. На зовнішній поверхні стіни, що виходить на вулицю, кабінету керівника:
Візуальний огляд огорожувальних конструкцій (_ люд. годин).
 3. У приміщенні секретаря (суміжному з кабінетом керівника):
(наводиться перелік запланованих робіт)
 4. У приміщенні бухгалтерії:
(далі триває перелік приміщень, у тому числі суміжних з тим, що перевіряється, і перелік запланованих у них робіт).

Час проведення спеціальної перевірки:

З (дата, час) по (дата, час). Загальна тривалість безпосереднього проведення перевірки – _ годин.

Варіант прикриття попереднього огляду приміщень:

Огляд приміщень для складання кошторису на монтаж системи примусової вентиляції (з (дата, час) по (дата, час)). Доводиться під запис до секретаря та відповідального за експлуатацію будівлі за три дні до огляду (дата).

Документ, що підтверджує легенду – копія договору на виконання монтажних робіт.

Варіант прикриття пошукових робіт:

1. Перевірка спеціалістами телефонного вузла зв'язку, стану телефонних ліній та обладнання (з (дата, час) по (дата, час)). Доводиться під запис до секретаря за два дні до перевірки (дата).

Документи, що підтверджують легенду – наряд на проведення робіт та допуск для робіт на обладнанні.

2. Пошук контактів, що іскрять, прихованої електропроводки для усунення перешкод ПЕОМ (з (дата, час) по (дата, час)). Доводиться до

секретаря та відповідального за електрогосподарство перед перевіркою (дата).

Документ, що підтверджує прикриття – копія договору на виконання пошукових робіт.

Заходи по активації встановлених закладних пристроїв:

Доведення до секретаря і осіб керівного складу підприємства інформації про проведення у день перевірки наради керівного складу підприємства з питань прискорення розробки нових зразків продукції та просування їх на ринок товарів та послуг. Спосіб доведення – поширення серед осіб керівного складу повістки дня наради і розпорядження про підготовку доповідей. Дата проведення: __ (за тиждень до початку перевірки).

Дії у випадку виявлення засобів неявного знімання інформації:

Не чіпаючи виявлений засіб, доповісти про факт виявлення керівнику і начальнику служби безпеки підприємства для прийняття рішення про подальші дії.

3. Засоби і сили, що залучаються, їх розподіл по об'єктах і видах робіт.

Склад пошукової бригади:

1. _____ - керівник;
2. _____.
3. _____.

Перелік спеціального обладнання і технічних засобів, що залучаються до проведення перевірки:

1. Комплекс доглядових дзеркал (використовується тільки при зачинених дверях і приміщеннях і відсутності у ньому сторонніх осіб).
2. Пошуковий програмно-апаратний комплекс ПАК DigiScan (застосовується тільки при зачинених дверях приміщення і відсутності у ньому сторонніх осіб).
3. Пристрій нелінійної радіолокації NR 900E (у процесі радіомоніторингу не вмикати, використовувати тільки при зачинених дверях приміщення і відсутності у ньому сторонніх осіб).

(далі триває перелік обладнання і технічних засобів з вказанням основних особливостей їх застосування у рамках обраних варіантів прикриття та інших обмежень, встановлених умовами перевірки).

Додаткові заходи по активації встановлених ЗП:

У кабінеті керівника підприємства для активації ЗП з акустопуском з допомогою магнітоли відтворюється попередньо зроблені на науковій конференції записи доповідей. У приміщенні

бухгалтерії відтворюються попередньо записані записи не конфіденційних ділових питань. Початок відтворення записів – з початком проведення візуального огляду огорожувальних конструкцій, меблів та інших предметів інтер'єру приміщень.

При перевірці наявності сигналів у дротових лініях усе підключене до них обладнання приводиться у робочий стан (вмикається у робочий режим), трубки телефонних апаратів знімаються для переводу телефонних ліній у режим «зайнято».

4. Перелік звітних документів за результатами перевірки та термін їх представлення для затвердження.

1. Комплексної спеціальної перевірки приміщень.
2. Опис проведених робіт та досліджень.
3. Рекомендації по підвищенню надійності захисту інформації від її можливого витоку по технічних каналах.
4. Журнал реєстрації заводських та інвентарних номерів обладнання, меблів та предметів.
5. Журнал реєстрації пломб та прихованих міток.

Акт проведення перевірки приміщень – у двох екземплярах (один – виконувачам робіт). Інші документи у одному екземплярі.

Усі документи – з грифом «конфіденційно».

Термін подання для затвердження – _.

Погоджено

Керівник організації, що
проводить перевірку

_____/_____/

" ____ " _____ 20__ р.

Керівник пошукової бригади

_____/_____/

Члени пошукової бригади

_____/_____/

_____/_____/

" ____ " _____ 20__ р.

МЕТОДИКА ПОШУКУ ЗАКЛАДНИХ ПРИСТРОЇВ З ВИКОРИСТАННЯМ ПОШУКОВОГО ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ ПАК DIGISCAN

1. Призначення та складові комплексу.

Автоматизований пошуковий програмно-апаратний комплекс ПАК DigiScan, що складається з портативного комп'ютера із спеціальним програмним забезпеченням DigiScan-2000 і скануючого приймача AR-3000A, призначений для виявлення радіосигналів з закладних пристроїв, визначення їх частоти, смуги пропускання, дослідження сигналів по кореляційних функціях, амплітудних і спектральних характеристиках, виявлення гармонік сигналу, класифікації виявленого сигналу (дружній або небезпечний) і занесення результату у базу даних.

Комплекс DigiScan виявляє наступні види радіовипромінюючих закладних пристроїв як з відкритим каналом, так і з маскуванням інверсії спектру:

- кімнатні радіопередавачі з автономним живленням;
- кімнатні радіопередавачі з живленням від мережі, телефонної лінії або іншого джерела;
- переносні радіопередавачі;
- телефонні передавачі.

DigiScan дозволяє вести пошук як в потайному режимі, так і в активному режимі. У потайному режимі не видаються ніякі звукові сигнали, які демаскують роботу. Програма управляє підзвучкою приміщення, яка потрібна для активації закладних пристроїв з "ввімкненням по голосу" і для успішного виміру кореляції. В якості підзвучки використовується CD або MIDI-програвач.

У активному режимі забезпечується максимальна швидкість і надійність виявлення. Програмне забезпечення DigiScan-2000 керує звуковою картою для видачі звукових імпульсів або тональних посилок.

При вимірюванні кореляції програма порівнює сигнал із звукового виходу приймача і референтний сигнал. При схожості цих сигналів кореляція дорівнює 1 і сигнал вважається небезпечним. Як джерело референтного сигналу використовується активний мікрофон, який обладнаний кабелем, завдовжки 10 м, що дозволяє перевіряти також і прилеглі сусідні приміщення без переміщення комп'ютера.

Результати усіх тестів DigiScan підсумовує в єдиний рівень небезпеки (НЕБЕЗПЕКА), по якому робиться висновок про тип сигналу. Значення НЕБЕЗПЕКИ може набувати значення від 1 до 5. Рівень НЕБЕЗПЕКИ задає оператор.

Склад програмно-пошукового комплексу DigiScan:

- 1) Портативний комп'ютер;

- 2) Спеціалізоване програмне забезпечення DigiScan-2000;
- 3) Активні акустичні колонки до комп'ютера;
- 4) Скануючий радіоприймач AR 3000A;
- 5) Зовнішня антена приймача DA 3000;
- 6) Кабель з виносним мікрофоном та блоком живлення 12 В (рис. 1);
- 7) Сполучний кабель RS 232 від приймача AR 3000A до COM-порту комп'ютера.

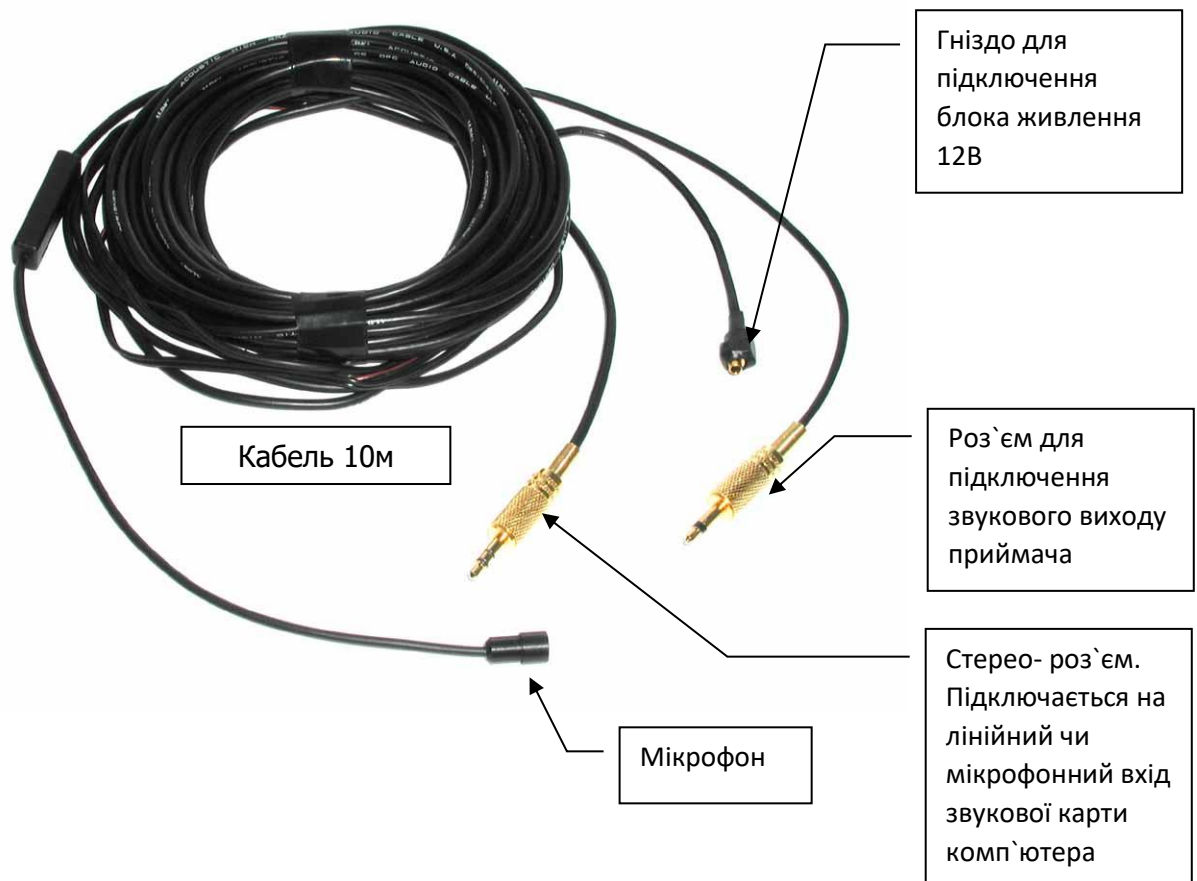


Рис. 1. Кабель з виносним мікрофоном.

2. Підготовка приміщення, яке перевіряється.

При підготовці до пошуку необхідно провести відповідно до плану (додаток 1) заходи по підготовці приміщення, що перевіряється, і по активізації встановлених ЗП, таких, що включаються дистанційно або за принципом акустопуска. В якості таких заходів може бути:

- організація "неправдивої" зустрічі або переговорів;
- відтворення на магнітофоні доповідей, записаних на відкритій нараді;
- ввімкнення усіх комп'ютерів, офісного устаткування, освітлення для створення робочої обстановки;
- зняття телефонних слухавок з апаратів, відключення радіотелефонів і інших санкціонованих радіопередавачів;
- відключення засобів технічного захисту інформації.

3. Підготовка комплексу до роботи.

Підготовка комплексу до роботи полягає в під'єднанні усіх кабелів, підключенні усіх апаратів і установці початкових налаштувань. Послідовність виконання робіт наступна:

- 1) встановити на робочому місці портативний комп'ютер і приймач AR – 3000A;
- 2) підключити акустичні колонки до виходу "SPK" звукової карти комп'ютера;
- 3) підключити роз'єм кабелю мікрофону в гніздо "LINE" комп'ютера;
- 4) підключити до гнізда живлення мікрофону блок живлення 12 В;
- 5) підключити роз'єм кабелю мікрофону до звукового виходу "EXT. SP" приймача AR – 3000A;
- 6) підключити сполучний кабель до роз'єму "REMOTE" приймача AR – 3000A і до COM- порту комп'ютера;
- 7) підключити зовнішню антену DA 3000 до роз'єму "ANT" приймача AR – 3000A;
- 8) підключити блок живлення 12 В до роз'єму "DC 12 V" приймача AR - 3000A;
- 9) підключити ключ HASP до порту LPT1 комп'ютера;
- 10) підключити до мережі 220В, 50 Гц блок живлення приймача AR – 3000A, блок живлення мікрофону і вилку шнура живлення комп'ютера;
- 11) встановити на AR – 3000A перемикач вбудованого ДК у положення "ON" (на задній панелі приладу);
- 12) встановити на приймачі AR – 3000A регулятор гучності "VOLUME" в позицію "10 година", регулятор чутливості "SQUELSH" в позицію "12 година";
- 13) включити живлення комп'ютера "POWER";
- 14) включити живлення приймача AR – 3000A ("POWER" - ON), на РКІ (рідкокристалічний індикатор) приймача з'явиться символ "RMT".

4. Запуск програми DigiScan-2000, встановлення порогу і параметрів сканування.

Після виконання усіх з'єднань і підключень (пункт 3), запуску операційної системи комп'ютера необхідно виконати запуск програмного забезпечення DigiScan-2000 (далі по тексту програми). Виконати команду "DigiScan-2000" в меню "Програми" кнопки "Пуск".

Після запуску програми відкривається вікно "Пошук приймача", автоматично виконується тестування підключеного приймача і встановлюються параметри з'єднання: швидкість обміну, порт та ін. (див. таблицю.1). Після цього відкривається головне вікно програми, що складається з:

- 1) меню команд: Файл, Режим, Тести, Сигнали;
- 2) панелі інструментів;
- 3) головної панорами (у лівому верхньому кутку екрану);
- 4) допоміжної панорами;

- 5) вікна бази даних сигналів;
- 6) вікна осцилограм і спектрограм;
- 7) вікна протоколу;
- 8) регулятора гучності.

Після цього необхідно задати поріг чутливості і параметри сканування.

Встановлення порогу.

Вікно встановлення порогу відкривається за допомогою команди «Поріг» з меню «Режим».

Поріг - це рівень, при перевищенні якого, поточна частота заноситься у базу даних і програма переходить в режим аналізу цього сигналу. Рівень порогу вибирається оператором, з урахуванням місцевої радіообстановки, залежно від рівня фонових шумів на ділянках діапазону, що перевіряється. Чим вищий поріг, тим вища швидкість пошуку і більша вірогідність пропуску сигналу. Чим менший поріг, тим надійність пошуку вища, але швидкість менша.

Для кожної ділянки діапазону частот необхідно виставити:

- початкову частоту ділянки діапазону «Початок F1»;
- кінцеву частоту ділянки діапазону «Кінець F2»;
- рівень порогу (від 0 до 15);
- значення атенюатора (0, - 10 або - 20 дБ).

Уся інформація про ділянки діапазону і виставлені рівні порогу і атенюатора зберігається у файлі ar3000.thr.

Встановлення параметрів.

У вікні параметрів задаються усі властивості і алгоритм роботи програми. Вікно параметрів відкривається командою «Параметри» з меню «Режим» і має 5 сторінок: «Приймач», «Пошук», «Аналіз», «Звук», «Сповідання». Встановлювані параметри і рекомендовані значення зведені в таблицю 1.

Встановлювані параметри роботи програми DigiScan

Таблиця 1

| <i>Налаштовувані параметри</i> | <i>Рекомендовані значення</i> |
|---------------------------------------|-------------------------------|
| Сторінка «Приймач» | |
| Приймач | AR-3000A |
| Адреса CI-V | 52 |
| Порт | COM2 |
| Швидкість обміну | 9600 |
| Інтервал опитування | 25 мс |
| Кількість запитів | 2 |
| Приймач підключений до звукової карти | Лінійний |
| Сторінка «Пошук» | |
| Діапазон: Почат, МГц | 20 |
| Кінець, МГц | 2000 |

| <i>Налаштовувані параметри</i> | <i>Рекомендовані значення</i> |
|---|-------------------------------|
| Стандартний крок дорівнює половині WFM, кГц | 180 |
| Поріг небезпеки (1...5) | 2 |
| Виявляти: Підозрілі сигнали | |
| Сторінка «Аналіз» | |
| Додатково в модуляції АМ | обрати |
| Перевіряти гармоніки | 2 і 3 |
| Кореляція: Нема, Пасивна, Пасивна з зондуванням, Активна | обрати Активну |
| Амплітудна або Спектральна | обрати обидві |
| Час кореляції, с | 5 |
| Сторінка «Звук» | |
| Автоматичне регулювання підсилення | обрати |
| Озвучування: Ні (прослуховувати приймач), Використовувати CD-програвач, Використовувати MIDI- програвач | Ні |
| Записувати звуковий зразок | встановити |
| Час запису, с | 3 |
| Сторінка «Сповідання» | |
| Сигналізувати про закладку: Нема, При виявленні, При виявленні з підтвердженням користувача | обрати «При виявленні» |
| Звуковий сигнал | обрати waf-файл |

5. Сканування радіочастотного діапазону для пошуку небезпечних сигналів.

Комплекс працює під управлінням універсального пошукового програмного забезпечення DigiScan - 2000, яке реалізує наступні передові методи виявлення :

- динамічний поріг;
- вимір смуги сигналу;
- перевірка наявності гармонік сигналу;
- пасивна кореляція;
- пасивна кореляція із зондуванням;
- активна амплітудна кореляція;
- активна спектральна кореляція;
- відбір сигналів по сумарному рівню небезпеки.

DigiScan - 2000 працює в двох режимах - Пошук і Ручний режим.

Після виставки параметрів *оператор вмикає режим автоматичного сканування в заданому діапазоні* (команда «Пошук» в меню «Режим»).

У режимі пошуку програма автоматично сканує заданий діапазон, знаходить сигнали, що перевищують заданий поріг, і виконує тести, які встановив оператор. Якщо виявлено небезпечний сигнал, програма сповіщає оператора звуковим сигналом або виводить повідомлення на екран і включає запис звукового зразка. Сигнал заноситься в розділ бази даних «Небезпечні». Усі інші сигнали заносяться в розділ бази даних «Нові». У розділ «Усі» потрапляють усі сигнали, незалежно від небезпеки. Після декількох сканувань усього діапазону оператор зупиняє пошук і переходить в ручний режим.

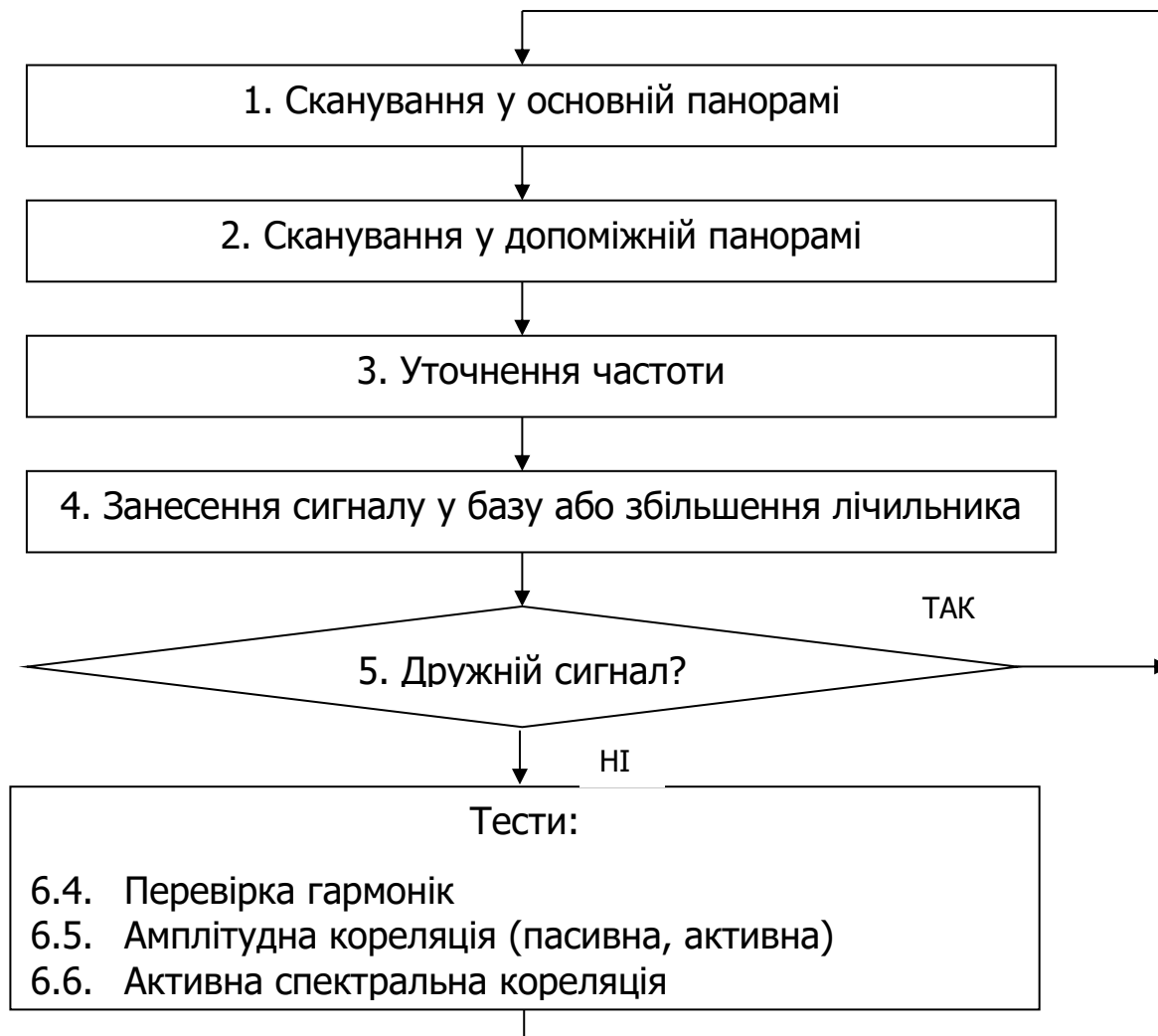


Рис. 2. Блок-схема алгоритму пошуку

У *ручному режимі* оператор може проаналізувати результати пошуку або спробувати самостійно знайти нові сигнали. Для цього оператор крокує по діапазону і виконує тести над виявленими сигналами. У ручному режимі також використовується поріг, що задається оператором. У ручному режимі оператор може переглядати осцилограму і спектр сигналів на дисплеях «Амплітуда» і «Спектр».

Алгоритм пошуку небезпечних сигналів.

Алгоритм пошуку небезпечних сигналів зображений на блок-схемі, представлений на рис. 2. Поточна операція відображається в рядку статусу внизу програми.

Скандування в основній панорамі.

У режимі пошуку DigiScan - 2000 починає скандування в головній панорамі. Модуляція приймача - WFM, крок скандування дорівнює смузі цієї модуляції. Для AR3000A ця величина складає 180 кГц. Синя вертикальна лінія на основній панорамі - це маркер, який показує поточну частоту. На головній панорамі червоною лінією відображається поріг. При перевищенні порогу

програма запам'ятовує частоту, на якій почалося перевищення (F1) і продовжує сканування до частоти, на якій перевищення закінчується (F2). Програма запам'ятовує ці частоти і переходить до детального сканування в допоміжній панорамі.

Основна панорама дозволяє відобразити від 0.1% до 100% діапазону, що перевіряється. Для масштабування використовується регулятор в нижній лівій частині основної панорами. Перед початком пошуку, коли задаватиметься поріг, рекомендується встановити масштаб 50-100% для перегляду усього діапазону.

Редагування порогу здійснюється до початку пошуку за допомогою команди «Поріг» пункту меню «Режим».

Сканування в допоміжній панорамі.

Модуляція приймача - NFM, крок сканування дорівнює смузі цієї модуляції. Для AR3000A ця величина складає 12 кГц. Маркер поточної частоти відображається синьою вертикальною лінією. Діапазон сканування в допоміжній панорамі (f1, f2) автоматично обчислюється по значенням частот F1 і F2 :

- початок діапазону $f1 = F1 - 90$ кГц;
- кінець діапазону $f2 = F2 + 90$ кГц.

Після того, як програма закінчить сканування в діапазоні від f1 до f2, вона переходить до пошуку перевищень порогу. Виявлені сигнали програма заносить у список, вибирає перший сигнал з цього списку і переходить в режим уточнення частоти цього сигналу.

Допоміжна панорама дозволяє відобразити від 0.1% до 100% діапазону, що перевіряється. Для масштабування використовується регулятор в нижній лівій частині основної панорами.

Уточнення частоти.

У цьому режимі DigiScan - 2000 уточнює частоту сигналу зі списку, отриманого під час детального сканування. Сканування у допоміжній панорамі проводилося з кроком, рівним смузі NFM – 12 кГц. Закладка може мати частоту, зміщену відносно 12кГц сітки і програма може неточно настроїтися і пропустити її. Щоб уникнути цього, програма перевіряє рівень сигналу на частоті, меншій на половину кроку NFM і більшій на половину кроку NFM. Якщо на якійсь з цих сусідніх частот рівень вищий, ніж на центральній частоті, то ця сусідня частота вважатиметься частотою сигналу. Таким чином, точність виміру частоти підвищується до 6 кГц.

Занесення сигналу у базу або збільшення лічильника.

Виявлені сигнали автоматично заносяться програмою у базу даних, незалежно від рівня небезпеки. Якщо сигнал вже є у базі даних, його лічильник збільшується на 1.

Пропуск дружніх сигналів.

Якщо сигнал вже є у базі даних і помічений як дружній, то процес пошуку пропускає цей сигнал і продовжує роботу по перевірці інших сигналів або скануванню. Дружні сигнали мають позначку «ДР» біля рівня небезпеки. При роботі в ручному режимі позначку «ДР» треба ставити вручну.

Примітка. Позначка сигналів як "дружніх" виключає їх з тестування під час пошуку. Необхідно точно упевнитися, що усі сигнали безпечні, інакше можна пропустити закладку.

Перевірка гармонік.

У цьому режимі DigiScan - 2000 перевіряє наявність 2-ої і 3-ої гармоніки сигналу. Через обмеження в об'ємі і потужності закладки, а також близькості до її антени, сигнал може мати гармоніки, кратні основній частоті. Наявність гармонік підвищує рівень небезпеки сигналу.

Знаючи основну частоту сигналу, програма обчислює частоти гармонік, множивши основну частоту на 2 (2-а гармоніка) і на 3 (3-я гармоніка). Після цього на приймачі встановлюється модуляція WFM, він налаштовується на частоти гармонік, і робиться зчитування рівня на цих частотах. Якщо рівень сигналу на цих частотах перевищує поріг, то вважається, що частота має гармоніки.

Якщо частота має обидві гармоніки, то сумарний рівень небезпеки сигналу підвищується на 1. Якщо гармонік немає або є одна з двох, то рівень небезпеки не підвищується.

Якщо налаштуватися на частоту гармоніки в ручному режимі, то можна почути такий же звук як на основній частоті, тільки з деякими спотвореннями.

Для повноти аналізу рекомендується завжди встановлювати перевірку гармонік. Якщо діапазон, що перевіряється, розпочинається з частоти вище 1000 МГц, то перевірка 3-ої гармоніки не має сенсу, оскільки частота 3-ої гармоніки буде вища за верхній діапазон приймача. При накопиченні бази цих дружніх сигналів рекомендується відключати перевірку гармонік.

Амплітудна кореляція.

У цьому режимі програма вимірює зв'язок між акустикою приміщення, що перевіряється, і сигналом на звуковому виході приймача, який називається кореляцією (К). При амплітудній кореляції йде порівняння амплітуди сигналу в часі. Для аналізу акустики приміщення використовується активний референтний мікрофон, що входить в комплекс. Кореляція (коефіцієнт кореляції) може знаходитися в діапазоні від - 1 до +1. Якщо зв'язок між акустикою приміщення і сигналом на виході приймача є, то кореляція буде близька до +1. Така кореляція говорить про те, що приймач налаштований на закладний пристрій.

У режимі пошуку амплітудна кореляція робиться при декількох видах модуляції - WFM, NFM і AM (встановлюється перед включенням режиму пошуку).

Результати виміру кореляції відображаються в правій нижній частині головного вікна DigiScan - 2000 на сторінці «Протокол». Амплітудна кореляція позначається K1. У базу даних потрапляє максимальне значення кореляції при модуляції WFM, NFM і AM і зберігається в полі K1.

Відповідно до значення K1 обчислюється рівень небезпеки перевіреного сигналу :

- при $K1 = 0-0,33$, рівень небезпеки не змінюється;
- при $K1 = 0,33-0,66$, рівень небезпеки підвищується на 1;

- при $K1 = 0,66-1,0$, рівень небезпеки підвищується на 2.

Залежно від умов, в яких проводиться перевірка, *можна використати один з видів амплітудної кореляції:*

- пасивна;
- пасивна із зондуванням;
- активна;

Пасивна кореляція.

Пасивна кореляція робиться беззвучно і не демаскує пошуковий захід. Для успішного проведення пасивної кореляції в приміщенні має бути якийсь звук. Це може бути музика з CD- або MIDI-програвача комп'ютера, запис курсу англійської мови на касеті або радіоприймач. Якщо використовується радіоприймач, то частота, на яку він налаштований, може бути занесена програмою в розділ «Небезпечні». Пасивна кореляція дає менш точні результати, ніж активна. Наприклад, якщо в активному режимі кореляція закладки дорівнює 0.76, то в пасивному вона може бути 0.45, а іноді і менше. Якщо кількість проходів діапазону більше одного, то вірогідність пропуску небезпечного сигналу зменшується. Для підвищення точності виміру пасивної кореляції необхідно задавати час кореляції більшим, ніж при проведенні активної. Для пасивної кореляції рекомендується виставляти час не менше 10 секунд.

Для озвучування приміщення можна використати CD- або MIDI-програвач комп'ютера. Установка цих параметрів виконується на сторінці «Звук» команди «Параметри» в меню «Режим».

Пасивна кореляція із зондуванням.

Той же тест, що і для пасивної кореляції, за винятком того, що програма під час виміру кореляції періодично міняє гучність CD - або MIDI- програвача. Спочатку гучність стає максимальною, потім мінімальною і так далі. Це дозволяє значно підвищити точність кореляції і не демаскувати процес пошуку. Суб'єкт, який прослуховує закладку, може подумати, що просто йде налаштування гучності. Такий вид кореляції вимагає використання озвучування за допомогою CD - або MIDI- програвача комп'ютера. Час пасивної кореляції із зондуванням може бути 5-10 секунд.

Активна амплітудна кореляція.

Під час активної амплітудної кореляції DigiScan - 2000 також порівнює амплітуду акустики приміщення і сигналу із звукового виходу приймача. Відмінність полягає в тому, що під час активної кореляції колонки комп'ютера відтворюють звукові імпульси, які значно підвищують точність і надійність пошуку. Звукові імпульси відтворюються з випадковим періодом від 0.2 до 1 с. При використанні активної кореляції час може бути менший (3-5 с), хоча для підвищення надійності можна встановити і більше.

Спектральна кореляція.

У цьому режимі програма порівнює спектр акустики приміщення і сигналу із звукового виходу приймача. Для успішного проведення спектральної кореляції необхідно, щоб в приміщенні звучав тональний сигнал з частотою, що змінюється. Це досягається відтворенням звукового файлу

default.wav з таким сигналом. Час кореляції залежить від довжини цього файлу.

Спектральна кореляція також робиться при декількох видах модуляції - WFM, NFM і AM. Результати спектральної кореляції відображаються в закладці «Аналіз» головного вікна в колонці K2. Таке ж ім'я має поле бази даних, в якому зберігається максимальний результат кореляції (при різній модуляції).

Коли спектральна кореляція близька до $k-1$, це означає що є зворотний зв'язок між спектром звуку в приміщенні і спектром сигналу, що приймається. Це можливо при використанні радіопередавачів з інверсією спектру.

Відповідно до значення K2 обчислюється рівень небезпеки перевіреного сигналу:

- при $K2= 0-0.33$, рівень небезпеки не змінюється;
- при $K2 0,33-0.66$, рівень небезпеки підвищується на 1;
- при $K2= 0,66-1,0$, рівень небезпеки підвищується на 2.

Загальний рівень небезпеки сигналу обчислюється по наявності гармонік і по коефіцієнтах амплітудної і спектральної кореляції. При перевищенні рівня небезпеки порогового значення (рекомендоване значення 2), сигнал класифікується як небезпечний і заноситься у базу небезпечних сигналів.

Аналіз результатів пошуку.

Після декількох проходів і сканування заданого діапазону частот можна роздрукувати усю базу або базу небезпечних сигналів, в якій записані наступні параметри сигналів:

- частота, модуляція, смуга;
- наявність гармонік;
- значення $K1$ і $K2$;
- загальний рівень небезпеки;
- час, дата занесення сигналу у базу;
- значення лічильника (скільки разів сигнал зустрічався в процесі пошуку);
- коментар.

База даних має наступні розділи: «Нові», «Небезпечні», «Дружні», «Усі».

Після цього детально аналізуються усі небезпечні сигнали в ручному режимі:

- прослуховується небезпечний сигнал;
- записується сигнал в waf- файл;
- аналізується осцилограма;
- аналізується спектрограма;
- прослуховується 2-а і 3-я гармоніки;
- обчислюється коефіцієнт амплітудної кореляції;
- обчислюється коефіцієнт спектральної кореляції.

На основі детального аналізу небезпечних сигналів *робиться висновок* про наявність в приміщенні, що перевіряється радіовипромінюючого закладного пристрою і його характеристик.

Усі результати роботи автоматично заносяться у файл протоколу, який є звітним документом. Надрукований протокол додається до акту перевірки (додаток. 6). Крім того, до звітних документів відносяться база небезпечних сигналів, осцилограми, спектрограми сигналів виявлених закладних пристроїв.

Локалізація і пошук місця розташування виявлених радіопередавальних ЗП виконується за допомогою додаткових пошукових засобів:

- ST 031 «Піранья»;
- PROTECT 2103;
- RFM-32.

Додаток 3

МЕТОДИКА ПОШУКУ ЗАКЛАДНИХ ПРИСТРОЇВ З ВИКОРИСТАННЯМ ПОШУКОВОГО ПРИЛАДУ ST 031 «ПІРАНЬЯ»

1. Призначення.

Багатофункціональний пошуковий прилад ST 031 «Піранья» призначений для виявлення і локалізації спеціальних технічних засобів неявного добування інформації (закладних пристроїв), для виявлення природних і штучно створених каналів витоку інформації, а також для контролю якості захисту інформації. Він забезпечує рішення контрольно-пошукових завдань в межах приміщення (об'єкту) або у безпосередній близькості до нього.

Прилад може функціонувати в наступних режимах:

- 1) високочастотного детектора-частотоміра (RADIO - FREQUENCY CHANNEL) - для пошуку радіовипромінюючих ЗП;
- 2) скануючі аналізатори дротяних ліній (WIRE LINES ANALYSIS) - для пошуку ЗП, що використовують дровові лінії;
- 3) детектори інфрачервоних випромінювань (INFRARED CHANNEL) - для пошуку ЗП, що використовують інфрачервоне випромінювання;
- 4) детектори низькочастотних магнітних полів (MAGNETIC CHANNEL) - для пошуку ЗП, що використовують низькочастотні випромінювання;
- 5) віброакустичного приймача (VIBRO - ACOUSTIC CHANNEL) - для дослідження приміщень на предмет наявності віброакустичного каналу витоку інформації;
- 6) акустичного приймача (ACOUSTIC CHANNEL) - для дослідження приміщень на предмет наявності акустичного каналу витоку інформації.

Переведення приладу ST 031 «Піранья» у будь-який з режимів здійснюється автоматично при підключенні додаткових зовнішніх пристроїв (антен, адаптера, датчиків, мікрофону) до високочастотного роз'єму «RF ANT» або «PROBES». Одночасно прилад може працювати тільки в одному з перерахованих основних режимів.

2. Склад комплекту пошукового приладу ST 031 «Піранья».

До складу приладу входять наступні комплектуючі (рис. 1):

1. Основний блок керування, обробки і індикації.
2. Адаптер аналізатора дротяних ліній з приладом послаблення сигналів і світлодіодними індикаторами наявності напруги в лінії, яка перевіряється.
3. Насадки до адаптера (типу «Голка»).
4. Насадки до адаптера (типу «220 В»).
5. Насадки до адаптера (типу «Крокодил»).
6. Навушники.
7. Магнітна антена детектора низькочастотних магнітних полів з облаштуванням для забезпечення диференціального режиму роботи.
8. Високочастотна антена детектора-частотоміра.
9. З'єднувальний кабель для підключення магнітної антени і інфрачервоного датчика.
10. Виносний мікрофон акустичного приймача.
11. Інфрачервоний датчик детектора інфрачервоних випромінювань.
12. Виносний датчик віброакустичного приймача.
13. Телескопічна антена детектора-частотоміра.
14. Перехідник до телескопічної антени.
15. Наплічний ремінь основного блоку.
16. Підставка для основного блоку.
17. Блок живлення.



Рис. 1. Зовнішній вигляд комплектуючих приладу ST 031 «Піранья»

3. Конструкція та органи керування приладу ST 031.

Основний блок керування, обробки і індикації приладу ST 031 «Піранья» конструктивно виконаний у вигляді малогабаритного переносного моноблока. На передній панелі розташовані екран рідкокристалічного дисплея, органи керування і 16-ти кнопкова клавіатура, що забезпечує управління приладом в усіх режимах. Усі кнопки клавіатури управління є багатофункціональними.

Порядок їх використання і функції, що реалізуються при цьому, визначається особливостями роботи приладу в кожному з передбачених режимів.

В той же час, більшість кнопок управління забезпечують реалізацію первинних функцій, загальних для усіх режимів роботи. Зокрема:

- кнопка «MUTE» здійснює включення (виключення) вбудованого гучномовця;

- кнопка «HELP» дозволяє отримати при роботі у будь-якому режимі контекстну екранну допомогу з можливістю переміщення тексту натисненням кнопок «Δ» і «∇»;
- кнопка «OSC» вмикає осцилографічний контроль параметрів сигналу у поточному режимі;
- кнопка «SA» вмикає спектральний контроль параметрів сигналу в поточному режимі;
- кнопка «SAVE» забезпечує запис в енергонезалежну пам'ять виведеної на дисплей осцилограми або спектрограми з супутніми параметрами аналізованого сигналу;
- кнопка «LOAD» здійснює виклик на екран з енергонезалежної пам'яті раніше збереженої осцилограми або спектрограми;
- кнопка «RUN/STOP» робить пуск (зупинку) поточних динамічних вимірів параметрів контрольованого сигналу;
- кнопка «SET» дозволяє здійснювати вибір різних варіантів проведення аналізу контрольованого сигналу;
- кнопка «ENTER» забезпечує виведення для слухового контролю тонального сигналу, або того, що демодулюється;
- кнопка «RESET» перезапускає прилад.

Другі, а у ряді випадків і подальші, функції кнопок управління знаходяться в прямій залежності від особливостей застосування приладу у різних режимах.

У нижній частині передньої панелі розміщені перемикач живлення «OFF POWER ON», гніздо лінійного виходу «LINE» і гніздо підключення навушників «PHONE».

На верхній поверхні блоку розміщені три роз'єми. Роз'єм «RF ANT» служить для підключення телескопічної (через перехідник) або високочастотної антени детектора-частотоміра. Через роз'єм «PROBES» підключаються усі інші додаткові зовнішні пристрої, що входять в комплект приладу. Роз'єм «OSC2» призначений для забезпечення роботи вбудованого осцилографа і аналізатора спектру в двоканальному режимі, а також для реалізації можливості роботи приладу в якості звичайного низькочастотного одноканального осцилографа і аналізатора спектру.

На задній поверхні приладу розміщені вбудований гучномовець і батарейний відсік для 4-х елементів живлення (батарей) або акумуляторів типу AA. На нижній поверхні основного блоку розміщений роз'єм блоку живлення і різьбовий отвір для під'єднання підставки для основного блоку. На бічних стінках, у верхній частині розміщені різьбові отвори для під'єднання наплічного рем'я.

4. Підготовка приладу ST 031 до роботи.

Підготовку приладу ST 031 «Піранія» до роботи, особливо після тривалої перерви, доцільно розпочати із зовнішнього огляду - переконатися в цілісності сумки - упаковки, перевірити комплектність виробу і відсутність видимих механічних ушкоджень.

Підготувати джерела живлення. Для цього перевірити зовнішній стан батарей або акумуляторів на відсутність окислення на контактній поверхні полюсів. Виміряти вольтметром напругу кожного елемента живлення (повинно бути 1,45...1,55 В). Переконайтеся в механічній цілісності нерухомих і пружинних контактів, а також у відсутності на них слідів окислення. Вставити батареї або акумулятори, дотримуючись правильної полярності. Прилад готовий до включення і перевірки працездатності.

Після тривалої перерви в експлуатації приладу необхідно виконати наступні перевірки працездатності трактів:

- системи включення приладу і індикації стану джерела живлення;
- рідкокристалічного дисплея і підсвічування його екрану;
- системи автоматичного переведення приладу в основні режими;
- приватних трактів, що відповідають основним режимам приладу;
- звукового тракту;
- вбудованого низькочастотного осцилографа;
- вбудованого низькочастотного аналізатора спектру;
- енергонезалежної пам'яті.

Порядок перевірки і технологія викладені в Керівництві по експлуатації приладу ST 031.

5. Пошук радіовипромінюючих ЗП з допомогою приладу ST 031 у режимі високочастотного детектора-частотоміра (RADIO-FREQUENCY CHANNEL).

5.1. Порядок керування приладом у режимі високочастотного детектора-частотоміра.

Підключити телескопічну антену, використовуючи перехідник, або високочастотну антену до роз'єму «RF ANT». Включити живлення приладу.

Установка «нульового» порогу приладу здійснюється при ввімкненні автоматично. У разі потреби, натисненням кнопок «<» чи «>» встановити поріг детектора вручну, керуючись показаннями додаткової шкали «min - - -| - - - max». Якщо знадобиться, натисненням кнопки «Δ» повернутися до автоматичної установки порогу. Зниження порогу обов'язково призведе до частих неправдивих спрацьовувань індикації, а його завищення - до вірогідного пропуску сигналу «радіозакладки». І те, і інше значно ускладнює роботу оператора, збільшує час і знижує достовірність результатів перевірки. Тому для установки «нульового» порогу необхідно обов'язково дотримуватися декількох простих правил:

- не можна проводити установку порогу в приміщенні, що перевіряється, оскільки при функціонуванні у ньому вже розміщеної «радіозакладки», рівень її радіовипромінювання буде визначений приладом як «нульовий»;
- під час налаштування порогу неприпустимо використання радіостанцій, радіотелефонів і інших радіовипромінюючих засобів;

- не наближати антену приладу до включених ПЕОМ і інших засобів оргтехніки, як джерел ПЕМІ в діапазоні роботи приладу;
- не допускати контакту антени приладу з металевими предметами і дротами, як джерелами перевипромінених високочастотних сигналів;
- налаштування приладу слід робити в одному з найближчих приміщень, в якому, імовірно, рівень фону істотно не відрізняється, а встановлення «радіозакладок» або неможливе, або недоцільне. В якості таких приміщень зазвичай розглядають приміщення іншого призначення, але розташовані на тому ж поверсі і з віконними отворами, що виходять на ту ж сторону будівлі;
- якщо об'єктом перевірки є автомобіль або інший транспортний засіб, то, забезпечивши правильний вибір місця робіт, налаштування «нульового» порогу слід проводити не ближче 10 - 20 м від нього.

Після установки «нульового» порогу прилад переміщують в контрольоване приміщення (до контрольованого об'єкту) БЕЗ ВИМКНЕННЯ ЖИВЛЕННЯ. Бо кожне подальше його включення призводить до автоматичної установки порогу вже стосовно нових умов електромагнітної обстановки.

Візуально по кількості повністю забарвлених елементів індикаторів рівня сигналу і «на слух» по частоті клацань у вбудованому гучномовці або навушниках оцінити рівень сигналу, що приймається.

При необхідності натисненням кнопки «SET» встановити потрібні межі динамічного діапазону : (-8...-16) дБ; (- 8...-32)дБ; (- 8...-48)дБ.

Кнопкою «RUN/STOP» запускати і зупиняти динамічні виміри рівня і частоти радіосигналу.

Натисненням кнопки «ENTER» (переведення звукової індикації в режим «AUD») здійснювати прослуховування наявності і змісту потенційно небезпечних модульованих радіовипромінювань.

Натисненням кнопок «+» та «-» встановити необхідну гучність звукового сигналу (тонального або такого, що демодулюється), що виводиться на вбудований гучномовець, або на навушники.

Натисненням кнопки «OSC» перейти до осцилографічного контролю параметрів сигналу.

Натисненням кнопки «SA» перейти до аналізу спектру сигналу, що демодулюється.

У разі збоїв в роботі натиснути кнопку «RESET» і здійснити перезапуск приладу.

5.2. Використовувані методи пошуку і локалізації джерел радіосигналів.

Канали витоку інформації в радіочастотному діапазоні можуть бути створені штучно (навмисно), за рахунок використання зловмисниками спеціальних технічних засобів (радіомікрофони, телефонні

радіоретранслятори, несанкціоновано включені радіостанції, радіомаяки і т. д.). Вони можуть виникнути і природно, за рахунок побічних електромагнітних випромінювань (ПЕМВ) технічних засобів обробки інформації (ПЕОМ, телекси, факси і тому подібне).

У будь-якому випадку виникає необхідність класифікації сигналів в радіочастотному діапазоні по сукупності критеріїв на небезпечні і безпечні, на внутрішні і зовнішні.

Небезпечні радіосигнали можуть бути створені як внутрішніми, так і зовнішніми джерелами. Більше того, на практиці зустрічається досить велика кількість їх найрізноманітніших поєднань. Зазвичай до чисто внутрішніх небезпечних радіосигналів відносять:

- сигнали "радіозакладок" (радіомікрофони, телефонні радіотранслятори і тому подібне);
- сигнали радіомаяків;
- сигнали несанкціоновано включених в приміщенні радіостанцій та радіотелефонів;
- побічні електромагнітні випромінювання ПЕОМ і інших технічних засобів обробки інформації.

До категорії небезпечних, у поєднанні внутрішньо-зовнішні, прийнято відносити радіосигнали, джерелами яких можуть бути:

- радіомікрофони з виносним акустичним мікрофоном;
- телефонні радіоретранслятори, встановлені на лінії зв'язку за межами приміщення (але поблизу нього);
- радіостетоскопи, встановлені із зовнішнього боку поверхонь, що захищають приміщення;
- винесені передавачі прихованих відеокамер;
- пристрої зовнішнього високочастотного опромінення.

При роботі з приладом ST 031 «Піранья» використовують окремо або в поєднанні два основні методи пошуку і локалізації джерел небезпечних радіосигналів. Ними є так звані «Амплітудний метод» і метод «Акустичної зв'язки».

«Амплітудний метод» ґрунтується на різкому зростанні рівня сигналу, що приймається, при наближенні приймальної антени приладу до місця розташування його джерела. Радіус зони виявлення джерела залежить від потужності випромінюваного ним сигналу, спрямованості його антени і рівня фону електричного поля в точці розташування приймальної антени приладу.

Після фіксації факту виявлення потенційно небезпечного радіосигналу слід рухатися у напрямі зростання його рівня. Контроль за рівнем сигналу, що приймається, необхідно здійснювати за свідченнями індикаторів рівня на екрані дисплея приладу і по частоті клацань звукової сигналізації у режимі «TONE».

Метод «Акустичної зв'язки» ґрунтується на виникненні позитивного акустичного зворотного зв'язку між мікрофоном «радіозакладки» і динаміком приладу ST 031 «Піранья». Обов'язкове ввімкнення звукової сигналізації приладу в режим «AUD» для виведення на динамік сигналу, що

демодулюється. Ефект «акустичної зв'язки» виникає тільки відносно «радіозакладки», в якій застосовані звичайні види модуляції - амплітудна і частотна (вузькосмугова або широкосмугова). Причому у разі частотної модуляції ефект ґрунтується на наявності «паразитної» амплітудної модуляції в частотномодульованому сигналі (у разі якісно виконаної «радіозакладки» ефект «акустозв'язки» буде досить слабким, аж до повної відсутності).

Ознакою виникнення «акустозв'язки» є поява характерного «писку», тон і інтенсивність якого змінюються при наближенні динаміка приладу до мікрофону «радіозакладки». Слід враховувати, що наявність характерного звуку при використанні цього методу демаскує проведення робіт. Тому у разі застосування «радіозакладок» з дистанційним управлінням вони можуть бути вимкнені на час перевірки.

Раціональний вибір того або іншого методу багато в чому залежить від особливостей, властивих потенційно небезпечним радіосигналам і їх джерел.

5.3. Особливості проведення пошуку радіовипромінюючих ЗП.

Починаються роботи з підготовки контрольованого приміщення (об'єкту) і самого приладу ST 031 «Піранья».

Підготовка приміщення полягає в створенні умов, при яких забезпечується мінімально можливий рівень фону електричного поля. Це досягається відключенням засобів оргтехніки, ПЕОМ, перетворювачів і блоків живлення, базових станцій бездротових телефонів, люмінесцентних освітлювальних ламп і інших електронних пристроїв і електроприладів. Доцільно також закрити вікна і двері, опустити штори або жалюзі.

Особливо слід звернути увагу на те, щоб були вимкнені радіотелефони і інші радіопередавальні засоби, а також засоби активного радіотехнічного захисту, якщо ними обладнано приміщення, що перевіряється, або суміжні з ним. Не допускається одночасна робота приладу ST 031 «Піранья» з нелінійними локаторами.

Для створення акустичного фону і для активізації радіозакладок з акустопуском слід підготувати і розмістити в контрольованому приміщенні тестове джерело звуку - магнітофон з музичною або мовною фонограмою. Не рекомендується використати в цих цілях радіоприймач або телевізор.

Якщо об'єктом перевірки є автомобіль, то необхідно правильно вибрати, з точки зору зменшення рівня електромагнітного фону, місце проведення робіт. Так, поблизу нього не повинні знаходитися високовольтні лінії електропередачі, трансформаторні підстанції, випромінюючі засоби зв'язку, теле- і радіомовлення, а також великі відзеркалюючі поверхні – металеві огороження, стіни будинків, гаражі, інші автомобілі.

Підготовка приладу ST 031 «Піранья» (після перевірки його працездатності в цьому режимі) полягає в установці «нульового» порогу приладу (пункт 5.1), що є, фактично, визначальним для успішного проведення робіт.

Виконавши викладені вище правила і обмеження, можна рахувати приміщення (об'єкт), що перевіряється, і прилад ST 031 «Піранья» підготовленими до проведення контрольних-пошукових робіт.

Послідовність пошуку потенційно небезпечних радіосигналів і їх джерел полягає в перевірці наявності:

- автономних радіомікрофонів і телефонних радіоретрансляторів;
- радіомікрофонів, що камуфлюють, живляться від електромережі;
- радіостетоскопів;
- прихованих відеокамер з радіоканалом;
- просторового високочастотного випромінювання.

Пошук автономних радіомікрофонів і телефонних радіоретрансляторів доцільно здійснювати, відключивши від розеток електромережі шнури живлення усіх санкціонованих споживачів і вимкнути освітлювальні прилади з лампами розжарювання.

З урахуванням того, що радіочастотний тракт приладу ST 031 «Піранья» виконаний за поєднаною схемою детектора-частотоміра, для його застосування придатні ті ж прийоми і методи, як і для автономних детекторів поля, інтерсепторів та радіочастотомірів. В цілому вони полягають в наступному.

Якщо не накладаються обмеження на скритність проведення робіт, то найкращий ефект дає поєднання амплітудного методу і методу "акустозавязки". При проведенні потайного пошуку необхідно орієнтуватися на амплітудний метод з прослуховуванням детектованих сигналів через навушники.

Особлива увага звертається на радіовипромінювання в діапазоні 60 - 640 МГц, найбільш типовому для використання радіомікрофонами і телефонними радіоретрансляторами.

Пошук здійснюється шляхом планомірного обходу приміщення з рухом уздовж стін і обстеженням меблів і інших предметів. Зважаючи на досить велику чутливість високочастотної антени пошук доцільно починати із застосуванням телескопічної антени. При обході антenu необхідно орієнтувати в різних площинах, здійснюючи плавні, повільні повороти основного блоку і домагаючись максимального рівня сигналу. Антену приладу доцільно тримати на відстані не більше 20 - 25 см від обстежуваних поверхонь і предметів. За відсутності обмежень на використання методу «акустозав'язки» динамік вбудованого гучномовця приладу слід орієнтувати у бік обстежуваних поверхонь і предметів (значення гучності має бути встановлене на значення не менше 3/4 від максимального).

При наближенні антени до місця розміщення «радіозакладки» напруженість електромагнітного поля зростає, відповідно підвищується і рівень сигналу на його вході. З перевищенням рівня сигналу, встановленого «нульового» порогу, залежно від виду сигналу, збільшується кількість забарвлених секторів одного з рядків індикаторів рівня і, починаючи з четвертого (відлік від нульової відмітки), зростає частота клацань звукової сигналізації в режимі «TONE» - виникає «акустозав'язка».

У разі знаходження джерела з частотномодульованим сигналом збільшуватиметься кількість забарвлених секторів верхнього індикатора рівня сигналу. При достатньому наближенні до джерела радіочастотомір здійснює «захоплення» частоти і показує в останньому рядку екрану її значення за результатами декількох вимірів. Шляхом зменшення гучності кнопкою «-», зміни меж динамічного діапазону кнопкою «SET», збільшення вручну порогу спрацьовування детектора, постійного спостереження за свідченнями частотоміра звужується зона обстеження і, тим самим, локалізується місце встановлення «радіозакладки» з точністю 10 - 15 см. Додаткову можливість по класифікації радіовипромінювань дає періодичне включення режиму «AUD» і прослуховування демодульованого сигналу.

Проте, ефект «акустозав'язки» і виразне прослуховування сигналу, що демодулюється, спостерігаються не завжди. Наприклад, якщо закладки мають маскований радіоканал. Тому в основі їх пошуку лежить використання амплітудного методу в чистому вигляді. Доповнюючим тут може бути простий прийом. Якщо вимкнути джерело тестової фонограми і створити в приміщенні, що перевіряється, короткий різкий звук (сильний хлопок, удар по кришці столу або металевому предмету), то можна зафіксувати характерні зміни сигналу, що демодулюється, «на слух» в режимі «AUD», зміни осцилограми в режимі «OSC» і спектрограми у режимі «SA».

У разі застосування «радіозакладки» з цифровими методами модуляції індикація підвищення рівня відбуватиметься на нижньому індикаторі. Індикація частоти сигналу, що приймається, в даному випадку буде випадковою.

У разі застосування в якості «радіозакладки» телефонів стандарту DECT або GSM, окрім індикації підвищення рівня сигналу в нижньому рядку, на індикаторі з'явиться напис DECT або GSM.

Пошук телефонних радіоретрансляторів здійснюється аналогічно пошуку радіомікрофонів. При цьому для їх активізації необхідно зняти слухавки усіх телефонних апаратів. Власне пошук проводиться в два етапи.

Спочатку на наявність закладних пристроїв перевіряються самі телефонні апарати. Встановлений в апараті радіоретранслятор проявляється так само як і радіомікрофон. При наближенні антени приладу до такого телефонного апарату реагують засоби звукової (у режимі «TONE») індикації, індикатор рівня сигналу і частотомір. При перемиканні в режим «AUD» в динаміці або в навушниках прослуховується або безперервний, або переривчастий тональний сигнал телефонної станції. У ряді випадків при наближенні мікрофону телефонної трубки до динаміка приладу ST 031 може виникнути ефект «акустозав'язки». Не рекомендується перевіряти телефонні апарати в режимі гучномовного зв'язку (якщо він передбачений), оскільки в цьому випадку може виникнути неправдива «акустозав'язка» між мікрофоном і динаміком самого пристрою.

Далі пошук телефонних радіоретрансляторів здійснюється шляхом обходу приміщення уздовж абонентської телефонної лінії і виявлення на ній місць із зростанням (максимумом) рівня радіосигналу. При обході антену

приладу необхідно орієнтувати в різних площинах на мінімально можливій відстані від лінії. Практично завжди існує необхідність перевірки лінії аж до основного розподільного щита. Особливу увагу слід звертати на розподільні коробки і місця, де лінія прокладена прихованою проводкою. Встановлені на лінії телефонні радіоретранслятори локалізуються, в основному, амплітудним методом, що доповнюється перевіркою на виникнення «акустозав'язки».

Пошук замаскованих радіомікрофонів, що живляться від електромережі, і локалізація місця їх установки здійснюється тими ж методами, які були охарактеризовані вище. Для їх активізації необхідно увімкнути тестове джерело звуку. По черзі включити наявні освітлювальні прилади з лампами розжарювання і підключити до розеток електромережі шнури живлення санкціонованих споживачів. Послідовно провести обстеження кожного зі знову підключених засобів.

Пошук радіостетоскопів має певні особливості, обумовлені способами їх застосування (встановлення поза контрольованим приміщенням). Тому для виявлення сигналів радіостетоскопів необхідно обстежувати усі доступні зовнішні поверхні конструкцій, що захищають приміщення. Оскільки середовищем поширення віброакустичних коливань можуть бути труби опалювання і водопостачання, то перевірки підлягають і ці комунікації.

У переважній більшості радіостетоскопи використовують відкритий радіоканал. Це дає можливість аналізу прийнятого сигналу «на слух» в режимі «AUD». При перевірці конструкцій, що захищають приміщення, антену приладу слід розташовувати на мінімально можливій відстані від обстежуваних поверхонь, оскільки радіус зони виявлення сигналу від радіостетоскопа зазвичай менше, ніж від радіомікрофонів. При перевірці трубопровідних комунікацій необхідно виконувати ці ж рекомендації, але не допускати контакту антени з металевими поверхнями.

Локалізація радіостетоскопів здійснюється амплітудним методом в суміжних приміщеннях, що доповнюється, при необхідності, використанням режимів «OSC» та «SA».

Пошук прихованих відеокамер з радіоканалом передачі зображення (часто і звуку) зв'язаний з деякими труднощами, які визначаються подібністю сигналу відеопередавача з сигналом яскравості передавачів телевізійного мовлення і роботи значної кількості цих пристроїв в діапазоні телестанцій (від 60 до 500 МГц).

Тому в ході проведення робіт при виявленні такого сигналу першим є завдання його розпізнавання за критерієм «зовнішній-внутрішній». Для розпізнавання необхідно закрити вікна шторами або жалюзі, залишивши включеним внутрішнє освітлення. Зробити кілька разів включення і виключення штучного освітлення. При включеному режимі «AUD» повинні прослуховуватися виразні зміни тону продетектованого сигналу. Для підвищення надійності розпізнавання включити режим «OSC» і переконатися в зміні структури сигналу по осцилограмі при включенні і виключенні освітлення. Вид осцилограми радіосигналу передачі відеоінформації при різних значеннях параметрів горизонтальної розгортки показаний на рис. 2 і 3.

Якщо результати такої перевірки позитивні, то сигнал впевнено можна віднести до категорії внутрішніх, створених передавачем відеокамери, оскільки зміна освітленості приміщення на параметри сигналу телевізійного мовлення не впливає.

Принципово передавачі відеокамер можуть працювати на частотах до 2300 МГц. Виявлення сигналу (схожого на сигнал яскравості) на частотах поза діапазоном телевізійного мовлення практично однозначно свідчить про роботу передавача прихованої відеокамери. Локалізація таких засобів здійснюється амплітудним методом.

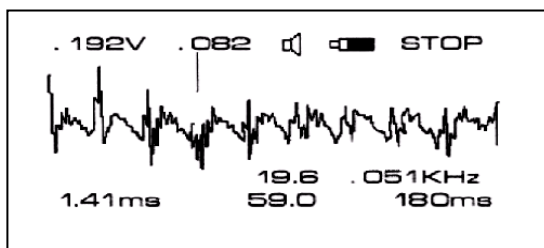


Рис.2. Радіосигнал передачі відеоінформації, період розгортки 180 мс

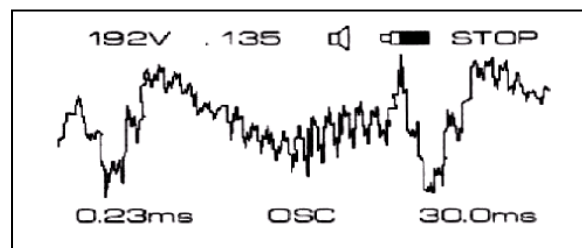


Рис.3. Радіосигнал передачі відеоінформації, період розгортки 30 мс.

Для виявлення просторового високочастотного опромінення основним є завдання виявлення факту створення цього штучного каналу добування інформації. Зазвичай воно вирішується в два етапи. На першому етапі виявляється факт опромінення приміщення високочастотним сигналом. На другому етапі відстежується відгук на зондуєчий високочастотний сигнал. При цьому необхідно орієнтуватися на наступні моменти.

Гостронаправлений промінь електромагнітної енергії може бути сформований тільки на дуже високих частотах (800...900 МГц і вище). Особливості поширення радіохвиль цього діапазону (необхідність «прямої видимості» між джерелом випромінювання і опромінюваними предметами) визначають в якості основних шляхів їх проникнення в контрольоване приміщення, передусім, віконні отвори. Об'єктами, що перевипромінюють, можуть бути звичайні для цього приміщення технічні засоби, що мають так званий мікрофонний ефект (паразитні акустоелектричні перетворювачі). До них зазвичай відносять динаміки побутових гучномовців, акустичні системи навіть вимкненої аудіоапаратури, телефонні апарати з електричним дзвінком і тому подібне. Перевипромінений на частотах вищих (найчастіше другою або третьою) гармонік сигнал локалізується у безпосередній близькості від опромінюваних предметів і має модуляцію акустичним фоном приміщення.

Виходячи з цього, може бути використаний наступний порядок роботи.

Для виявлення факту високочастотного опромінення по черзі обстежувати потенційно небезпечні віконні отвори. Для цього піднести антену до внутрішнього скла на відстань 5-10 см, зафіксувати рівень і частоту найбільш потужного сигналу. Увімкнути режим «AUD» і «на слух» визначити наявність і особливості сигналу, що демодулюється. По графічному

індикатору оцінити стабільність частоти випромінювання. Перейти у будь-яке з сусідніх приміщень (орієнтованих вікнами в ту ж сторону) і повторити перевірку в районі кожного з його віконних отворів. Високочастотне опромінення цілком вірогідне, якщо:

- частота сигналу, що приймається, лежить (чи дуже близька) в межах вказаного діапазону;
- стабільність частоти висока;
- модуляція сигналу відсутня;
- в сусідніх, по відношенню до того, що перевіряється, приміщеннях рівень сигналу, що приймається, значно менший.

Для виявлення джерел перевипромінювання необхідно ретельно обстежувати кожен з потенційно небезпечних предметів, розміщуючи антену приладу у безпосередній близькості до нього. Основою для ухвалення кінцевого рішення про опромінення і про наявність в приміщенні предметів, що перевипромінюють, є свідчення індикатора рівня приладу ST 031 «Піранья» і його частотоміра, а також результати прослуховування в режимі «AUD». При цьому в якості основних ознак зазвичай розглядають фіксацію номінала частоти, кратного третій гармоніці опромінюючого сигналу і ідентифікацію звукового сигналу в режимі «AUD» з акустичним фоном приміщення.

Методика пошуку і локалізації несанкціоновано ввімкнутих на передачу *радіостанцій, радіотелефонів, телефонів з радіоподовжувачами і радіомаяків* повністю аналогічна методиці пошуку і локалізації радіомікрофонів. Причому у переважній більшості випадків слід орієнтуватися на амплітудний метод з періодичним прослуховуванням сигналу, що демодулюється, в режимі «AUD».

6. Пошук ЗП, що використовують дротові лінії за допомогою приладу ST 031 в режимі скануючого аналізатора провідних ліній (WIRE LINES ANALYSIS).

6.1. Порядок управління приладом в режимі скануючого аналізатора провідних ліній.

Підключити мережевий адаптер до роз'єму «PROBES», а його щупи до дротової лінії (лінії електромережі з напругою до 600 В). Включити живлення приладу. Включиться режим скануючого аналізатора дротових ліній і на РКІ з'явиться напис «WIRE LINES ANALYSIS».

Дочекатися 2-х, 3-х кратного «проходу» діапазону сканування маркером в межах, що автоматично встановлюються, 0,1...10,450 МГц. При необхідності встановити найбільш раціональні межі частотного діапазону сканування:

- натиснути кнопку «SET», потім кнопку «4». Натисненням кнопок з цифровим маркуванням набрати число, що відповідає нижній межі діапазону. Натиснути кнопку «ENTER» і підтвердити завершення установки значення нижньої межі;

- натисненням кнопок з цифровим маркуванням набрати число, що відповідає верхній межі діапазону, натиснути кнопку «ENTER» для підтвердження установки верхньої межі діапазону.

Натиснути кнопку «<» або «>» і вибрати потрібний напрям і швидкість сканування.

Натиснути кнопку «SET», потім кнопку «3» до появи на екрані в четвертому рядку напису «3 - > ↑↓ THRESHOLD level».

Натиснути кнопку «ENTER» і повернутися на екран зображення панорами.

Натисненням кнопок «Δ» та «∇» встановити найбільш зручну межу індикації вимірника рівня сигналу (напис під горизонтальною віссю «level threshold = XX%»).

Натисненням кнопки «RUN/STOP» зупинити автосканування в необхідній точці частотної осі. Натисненням кнопок «<» або «>» провести точне ручне налаштування на частоту, що цікавить. Прослухати сигнал, що демодулюється. Натиснути кнопку «ENTER (AM/FM)» і обрати вид демодуляції («на слух», за якістю його відтворення). Натиснути кнопку «RUN/STOP» і повернутися до автосканування.

Включити систему автоматичної зупинки сканування на найбільш виражених (по амплітуді) частотних складових панорами.

Натиснути кнопку «SET», потім кнопкою «3» встановити в четвертому рядку меню напис «3 - > ↑↓ SQUELCH level». Натиснути кнопку «ENTER». Кнопками «Δ» і «∇» вибрати бажаний рівень автоматичної зупинки автосканування (по положенню короткої горизонтальної риски в правій частині екрану). Після зупинки сканування кнопками «<» та «>» зробити уточнення налаштування за ознакою якості сигналу, що демодулюється.

Для продовження сканування натиснути кнопку «RUN/STOP».

Ввімкнення режиму віднімання спектрів:

- натиснути кнопку «SET», потім кнопку «2» і встановити напис «2 -> Difference ON D2 – 1»;

- натиснути кнопку «ENTER» для початку процедури віднімання спектрів;

- вийти з режиму віднімання спектрів - натиснути кнопку «SET», потім кнопкою «2» і встановити напис «Difference OFF», натиснути кнопку «ENTER».

Запис зображення панорами в енергонезалежну пам'ять: натиснути кнопку «SAVE», потім «ENTER».

Перегляд у пам'яті і виведення на екран зображення панорами, що збережена раніше:

- натиснути кнопку «LOAD»;

- натиснути кнопку «RUN/STOP» і повернути на екран панораму, що динамічно відображається.

Видалення з пам'яті зображення якої-небудь панорами виконується натисненням кнопок «LOAD», потім «SAVE» і «ENTER».

Перехід до осцилографічного контролю параметрів здійснюється натисненням кнопки «OSC».

Перехід до аналізу спектру сигналу здійснюється натисненням кнопки «SA».

Перезапуск приладу у разі збоїв в роботі здійснюється натисненням кнопки «RESET».

6.2. Особливості пошуку ЗП, що використовують провідні комунікації.

Пошук таких ЗП полягає у виявленні штучно створених каналів витоку інформації по дротових лініях, в основі яких лежить використання спеціальних технічних засобів. Основними видами дротових ліній, для аналізу яких призначений прилад ST 031 «Піранья», є лінії електромережі, а також абонентські телефонні лінії і лінії систем пожежної і охоронної сигналізації.

В цілому прийоми і методи, використовувані для перевірки дротових ліній перелічених видів, однакові. Підключення до них здійснюється з використанням єдиного, універсального адаптера. Аналізу методом сканування піддається загальний діапазон частот від 0 до 15 МГц. Виведення результатів сканування робиться у вигляді зображення панорами з однотипним відображенням вимірних параметрів. Функції органів управління приладом однакові (незалежно від виду лінії, що перевіряється).

Загальні (для усіх ліній) положення методики роботи полягають у наступному.

Підготовка контрольованого приміщення полягає в перевірці відповідності кількості і призначення реально існуючих у ньому дротових ліній раніше виготовлених (представлених) у схемах їх прокладення.

Підготовка приладу ST 031 (після перевірки його працездатності в цьому режимі) фактично полягає тільки у виборі найбільш зручних наконечників до щупів, стосовно типу дротяних ліній, що перевіряються.

Найбільшу увагу слід приділяти діапазону частот 40 - 2500 кГц, як найбільш типовому для використання закладками, що живляться від напруги дротових ліній і передаючих перехоплену інформацію по їх дротах. Значно рідше зустрічаються закладні пристрої з частотами близько 7 МГц і вище. Для забезпечення гарантованої надійності непропуску сигналів закладок по частоті, верхня межа діапазону сканування в приладі ST 031 «Піранья» визначена на рівні 15 МГц.

Порядок дій оператора по виявленню ЗП.

Включити прилад. Дочекатися початку сканування в діапазоні до 10,450 МГц і після завершення 2-х, 3-х циклів встановити верхню межу діапазону на рівні 15 МГц. Уважно вивчивши найбільш характерні особливості зображення панорами визначити наявність частотних складових, що перевищують рівень загального фону.

При необхідності розбити діапазон на окремі інтервали і просканувати їх детально, зупиняючись, передусім, на частотах найбільш інтенсивних складових. Межі інтервалів задаються послідовним натисненням кнопок

«SET», «4», кнопок з цифровим маркуванням і кнопки «ENTER» (або альтернативний варіант із завданням центральної частоти і ширини смуги).

Встановити нижній поріг індикації рівня сигналу близько 10-15%. Для цього натиснути кнопку «SET», кнопкою «3» вивести напис «3 - > ↑↓ THRESHOLD level», натиснути кнопку «ENTER» і кнопками «Δ» та «∇» добитися установки цього порогу індикації. У подальшому, залежно від характеру зображення панорами, вибрати найбільш зручний для аналізу рівень порогу. Запуск і зупинка сканування здійснюється натисненням кнопки «RUN/STOP».

Після проходу декількох циклів сканування можна обґрунтовано встановити поріг «автозупинки» для чого натиснути кнопку «SET», обрати кнопкою «3» режим «SQUELCH LEVEL», підтвердити вибір кнопкою «ENTER» і, маніпулюючи кнопками «Δ» і «∇», поставити курсор на необхідний рівень. Після зупинки на частоті того або іншого сигналу слід зробити точне налаштування кнопками «<» і «>», одночасно аналізуючи сигнал «на слух» почерговим включенням детекторів «AM» і «FM» кнопкою «ENTER». Для аналізу слабких сигналів можна вибрати кнопками «SET», «5» і «ENTER» зручніший амплітудний діапазон (0,1 - 1,0 мВ).

При необхідності додаткового аналізу сигналів в дротових лініях перемкнути прилад у режими «OSC» або «SA», оскільки зображення осцилограм і спектрограм сигналів, що виводяться на екран дисплея, дають детальнішу характеристику параметрів. У цьому можна переконатися порівнявши зображення панорами і осцилограми одного і того ж цифрового сигналу передачі мовної інформації (рис.4 і рис.5).

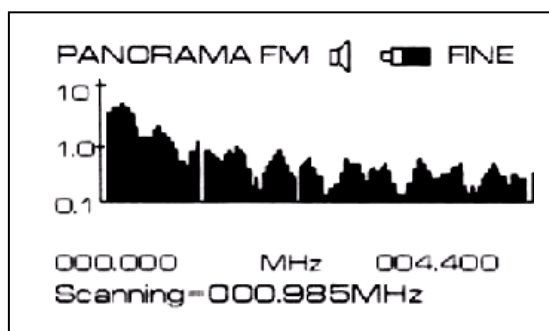


Рис.4. Панорама цифрового сигналу передачі мовної інформації у дротовій лінії.

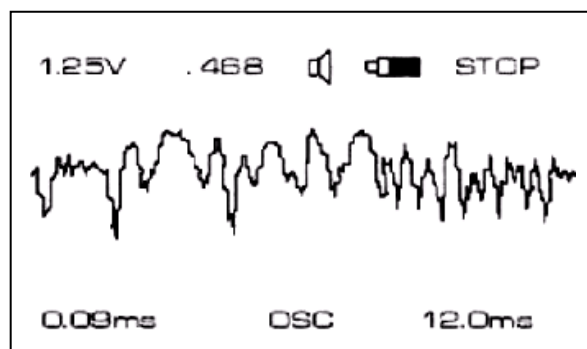


Рис.5. Осцилограма цифрового сигналу передачі мовної інформації у дротовій лінії (той самий сигнал)

Якщо у приміщенні регулярно проводяться перевірки, то доцільно зберегти в енергонезалежній пам'яті панораму (осцилограму, спектрограму) необхідних частотних інтервалів.

При пошуку ЗП в дротових лініях необхідно зважати на специфіку ліній кожного виду.

Перевірку наявності в електромережі ЗП, що приймають акустичні сигнали з приміщення, живляться від мережі і передають інформацію на

високій частоті по її дротах, доцільно розпочинати з мережевих розеток. Для зменшення рівня фону слід відключити (з видимим від'єднанням від розеток) усі електроприлади і апаратуру, розміщену в контрольованому приміщенні.

Підключити прилад до мережі, використовуючи для цього будь-яку з розеток.

Провести аналіз зображення панорами.

Якщо виявлений сигнал, що містить ознаки модуляції акустикою приміщення, то для локалізації його джерела може бути використаний метод «акустозав'язки», при почерговому підключенні до усіх розеток в приміщенні, що перевіряється.

Аналогічну перевірку провести на елементах ліній, що живлять електроосвітлювальні прилади.

Після перевірки силових ліній і ліній, що живлять освітлювальні прилади, необхідно перевірити трійники, подовжувачі і інші електроспоживаючі засоби шляхом їх почергового підключення до електромережі.

Перевірка дротових ліній систем пожежної і охоронної сигналізації, а також ліній невідомого призначення аналогічна перевірці ліній електромережі, оскільки аналогічні самі технічні засоби, що використовуються на цих комунікаціях.

При перевірці абонентських телефонних ліній, окрім пошуку описаних вище спеціальних технічних засобів, необхідно вирішувати задачу виявлення факту використання лінії для добування акустичної інформації з приміщення за рахунок лінійного високочастотного нав'язування. Ознакою факту лінійного високочастотного нав'язування є наявність в лінії немодульованого стабільного зонduючого сигналу на частотах не нижче 150 кГц. При цьому порядок підключення приладу і процедура аналізу не відрізняється від викладеного стосовно перевірки ліній електромережі.

Перевірка дротяних ліній систем пожежної і охоронної сигналізацій, а також ліній невідомого призначення аналогічна перевірці ліній електромережі, оскільки аналогічні самі технічні засоби, використововувані на цих комунікаціях.

При перевірці абонентських телефонних ліній, окрім пошуку описаних вище спеціальних технічних засобів, необхідно вирішувати задачу виявлення факту використання лінії для здобування акустичної інформації з приміщення за рахунок лінійного високочастотного нав'язування. Ознакою факту лінійного високочастотного нав'язування є наявність в лінії немодульованого стабільного зонduючого сигналу на частотах не нижче 150 кГц. При цьому порядок підключення приладу і процедура аналізу не відрізняється від викладеного стосовно перевірки ліній.

7. Пошук ЗП, що використовують низькочастотні магнітні випромінювання, за допомогою приладу ST 031 в режимі детектора низькочастотних магнітних полів (MAGNETIC CHANNEL).

7.1. Порядок управління приладом в режимі детектора низькочастотних магнітних полів.

Підключити зовнішню магнітну антену до сполучного кабелю, а сам кабель - до роз'єму «PROBES». Включити живлення приладу. Автоматично включиться режим детектора низькочастотних магнітних полів і на моніторі з'явиться напис «MAGNETIC CHANNEL». Осцилографічний контроль параметрів сигналу, що приймається по магнітному полю, включається автоматично.

Візуально по амплітуді і характеру сигналу на осцилограмі і «на слух» по його тональності у вбудованому гучномовці або навушниках оцінити рівень магнітного поля і присутність фону електромережі 220В, 50Гц або її гармонік. При необхідності, у разі високого рівня фону електромережі, включити диференціальний режим антени перемикачем на її корпусі (положення «до білої точки»).

Натисненням кнопки «RUN/STOP» запускати і зупиняти динамічні виміри.

Натисненням кнопки «MUTE» і кнопок «+» і «-» встановити необхідну гучність сигналу, що виводиться на вбудований гучномовець або на навушники.

Натисненням кнопки «SA» перейти до аналізу спектру прийнятого сигналу.

У разі збоїв в роботі натиснути кнопку «RESET» і здійснити перезапуск приладу.

7.2. Особливості проведення пошуку ЗП, що використовують низькочастотні магнітні поля.

У режимі детектора низькочастотних магнітних полів прилад ST 031 забезпечує прийом на зовнішню магнітну антену і відображення параметрів сигналів від джерел низькочастотних електромагнітних полів з переважаючою, (наявною) магнітною складовою поля в діапазоні від 300 до 5000 Гц.

Ідентифікація сигналів і їх джерел здійснюється на основі аналізу так, що автоматично виводиться на екран дисплея осцилограми, що відображає форму прийнятого сигналу і поточне значення його амплітуди. Підвищення достовірності ідентифікації сигналів і їх джерел забезпечується можливістю одночасного з аналізом зображення на екрані дисплея, прослуховування «фонові» обстановки з використанням вбудованого гучномовця або головних телефонів.

Особливістю низькочастотних магнітних каналів витоку інформації є те, що вони виникають при використанні по цільовому призначенню

санкціонованих засобів - ПЕОМ, переговорних пристроїв, систем звукопідсилення, магнітофонів, телефонів і так далі. Тому одним з основних завдань слід рахувати дослідження таких засобів на наявність, інтенсивність і дальність низькочастотного магнітного поля. Супутніми можуть вважатися завдання пошуку прихованої (несанкціоновано прокладеної) проводки і виявлення працюючих диктофонів.

Перед проведенням робіт доцільно вимкнути в приміщенні люмінесцентні світильники, а антену приладу, при необхідності, включити в диференціальному режимі.

Потенційні джерела небезпечних низькочастотних магнітних полів слід перевіряти окремо, включаючи їх в роботу по черзі.

При дослідженні *технічних засобів* необхідно оцінити дальність поширення магнітних полів і особливості їх спектру. Для цього спочатку розмістити магнітну антену у безпосередній близькості до досліджуваного об'єкту. Зафіксувати по осцилограмі відносний рівень поля. Віддаляючись від досліджуваного засобу і змінюючи просторову орієнтацію антени, оцінити дальність упевненого прийому низькочастотного сигналу.

Стосовно *підсилювачів звукової частоти*, що мають вихідний трансформатор, слід оцінити дальність упевненого (розбірливого) прийому мовного (тестового) сигналу. Така оцінка може послужити основою для правильного вибору місць установки відповідних засобів по відношенню до зовнішньої сторони приміщення і варіанту їх спільного розташування в приміщенні. При необхідності включити режим «SA», проаналізувати спектрограму і записати її в енергонезалежну пам'ять.

Для пошуку *прихованої проводки* необхідно послідовно обійти усі стіни приміщення, розташовуючи магнітну антену у безпосередній близькості до них. Зафіксувати область зростання рівня поля і шляхом переміщення антени по горизонталі і вертикалі визначити проходження траси прихованої проводки.

Можливість виявлення *працюючих диктофонів* визначається як рівнем магнітного поля, що створюється їх двигунами, так і рівнем магнітного фону приміщення. Для вирішення цього завдання зазвичай застосовують спеціалізовані засоби з попередньою ретельною підготовкою приміщення. Тому не завжди може бути досягнутий позитивний результат тільки при використанні приладу ST 031 «Піранья», особливо на відстані між диктофоном і магнітною антеною 30 см і більше.

8. Пошук ЗП, що використовують інфрачервоне випромінювання, за допомогою приладу ST 031 в режимі детектора інфрачервоних випромінювань (INFRARED CHANNEL).

8.1. Порядок управління приладом в режимі детектора інфрачервоних випромінювань

Підключити інфрачервоний датчик до сполучного кабелю, а сам кабель - до роз'єму «PROBES». Включити живлення приладу. Автоматично

включиться режим детектора інфрачервоних випромінювань і на моніторі з'явиться напис «INFRARED CHANNEL».

Установка «нульового» порогу детектора здійснюється при включенні автоматично. У разі потреби, натисненням кнопок «<» чи «>» встановити поріг детектора вручну, керуючись показаннями додаткової шкали «min - - -| - - - max». Якщо знадобиться, натисненням кнопки «Δ» повернутися до автоматичної установки порогу.

Візуально по кількості повністю забарвлених елементів 21-сегментної шкали і «на слух» по частоті клацань у вбудованому динаміку або навушниках оцінити рівень інфрачервоного випромінювання, що приймається.

Натисненням кнопки «RUN/STOP» запускати і зупиняти динамічні виміри рівня інфрачервоного випромінювання. Повторним натисненням цієї кнопки відновити динамічні виміри.

Натиснути кнопку «ENTER» (переведення звукової індикації в режим «AUD»), прослухати наявність і зміст потенційно небезпечних модульованих інфрачервоних радіовипромінювань.

Натисненням кнопки «MUTE» і кнопок «+» і «-» встановити необхідну гучність що виводиться або на вбудований динамік, або на навушники звукового сигналу (тонального або демодульованого).

Натисненням кнопки «OSC» перейти до осцилографічного контролю параметрів сигналу, що демодулюється.

Натисненням кнопки «SA» перейти до аналізу спектру сигналу, що демодулюється.

У разі збоїв в роботі натиснути кнопку «RESET» і здійснити перезапуск приладу.

8.2. Особливості пошуку ЗП, що використовують інфрачервоне випромінювання.

У режимі детектора інфрачервоних випромінювань прилад ST 031 забезпечує, з використанням виносного датчика, прийом випромінювань джерел інфрачервоного діапазону у ближній зоні, їх виявлення і виведення для слухового контролю і аналізу у вигляді тональних посилок (клацань), що чергуються або у вигляді явних фонограм при їх прослуховуванні. У кожен момент часу на тлі реальної обстановки перешкод приймається і виявляється найбільш потужний з усіх сигналів у робочому діапазоні.

При дослідженні джерел інфрачервоних випромінювань слід розглядати два види таких каналів витоку інформації. Один з них створюється за рахунок застосування спеціальних технічних засобів з передачею перехопленої інформації в інфрачервоному діапазоні. Інший канал ґрунтується на опроміненні скла віконних отворів спрямованим променем джерела інфрачервоних випромінювань і прийомі відбитого сигналу, що промодулюється акустикою приміщення.

Для виявлення обох каналів витоку необхідно провести однакові підготовчі заходи. Передусім слід правильно вибрати час проведення перевірки, а саме такий, коли у вікна контрольованого приміщення не

потрапляють прямі сонячні промені. У самому приміщенні необхідно вимкнути лампи розжарювання і джерела інтенсивного теплового випромінювання. Доцільно також вимкнути кольоровий телевізор, оскільки датчик приладу може реагувати на «теплі» тони зображення.

Специфіка інфрачервоних закладок зумовлює необхідність забезпечення «прямої видимості» між передавачем закладки і приймачем інфрачервоних випромінювань. Тому в приміщенні шлях проходження випромінювання передавача назовні може проходити тільки через віконні отвори. З урахуванням цих особливостей, пошук небезпечних сигналів слід починати від вікон приміщення, пересуваючись у його середину. Оскільки у передавача може бути досить вузька діаграма спрямованості, а точка зору датчика приладу складає 30° , необхідно плавно змінювати просторову орієнтацію датчика. Ознакою наявності інфрачервоного випромінювання є поява забарвлених сегментів шкали індикатора рівня і клацань звукової індикації в режимі «TONE» після забарвлення 4-го елемента шкали. Аналіз виявлених сигналів може бути виконаний «на слух» в режимі «AUD», а також візуально з використанням вбудованих осцилографа і аналізатора спектру. Локалізація джерел інфрачервоного випромінювання найточніше здійснюється поєднанням амплітудного методу і методу «акустозав'язки». При цьому порядок дій такий же як і при роботі в режимі височастотного детектора-частотоміра.

Для виявлення зовнішніх потенційно небезпечних інфрачервоних випромінювань необхідно обстежувати кожен віконний отвір. При цьому датчик орієнтується у бік вікна. Плавно змінюючи його просторове положення, провести обстеження усієї площі віконного отвору. Оскільки зондуючий сигнал не має модуляції, то його наявність може бути оцінена тільки за свідченнями індикатора рівня і тональної індикації в режимі «TONE».

9. Використання приладу для оцінки ефективності віброакустичного захисту і звукоізоляції приміщень

9.1. Порядок управління приладом в режимі віброакустичного приймача (у режимі акустичного приймача).

Підключити зовнішній віброакустичний датчик (виносний мікрофон) до роз'єму «PROBES». Включити живлення приладу. Автоматично включиться режим віброакустичного приймача (акустичного приймача) і на моніторі висвітлиться напис «VIBRO - ACOUSTIC CHANNEL» («ACOUSTIC CHANNEL»).

Осцилографічний контроль параметрів сигналу, що приймається по віброакустичному (акустичному) каналу, включається автоматично.

Візуально по амплітуді і характеру сигналу на осцилограмі і «на слух» по його розбірливості і якості у вбудованому динаміку або навушниках оцінити рівень і темброві характеристики перетвореного звукового сигналу.

Натисненням кнопки «RUN/STOP» запускати і зупиняти динамічні виміри.

Натисненням кнопки «MUTE» і кнопок «+» і «-» встановити необхідну гучність сигналу, що виводиться або на вбудований динамік, або на навушники.

Натисненням кнопки «SA» перейти до аналізу спектру прийнятого сигналу.

У разі збоїв в роботі натиснути кнопку «RESET» і здійснити перезапуск приладу.

9.2. Оцінка ефективності віброакустичного захисту і звукоізоляції приміщень.

У режимі віброакустичного приймача (акустичного приймача) прилад ST 031 забезпечує прийом від виносного віброакустичного датчика (від виносного мікрофону) і відображення параметрів низькочастотних акустичних сигналів в діапазоні 800-6000 Гц.

Стан віброакустичного захисту і звукоізоляції приміщення оцінюється як кількісно так і якісно. Кількісна оцінка здійснюється на основі аналізу осцилограми прийнятого сигналу і його амплітуди. Якісна оцінка ґрунтована на безпосередньому прослуховуванні прийнятого низькочастотного сигналу, аналізі його гучності і тембрових характеристик.

Об'єднання цих напрямів використання приладу визначається спільністю джерел виникнення каналів витоку інформації (мовний сигнал в акустичному діапазоні), схожістю прийомів контролю і практичною ідентичністю задіявання можливостей ST 031 «Піранья».

По-перше, і в тому, і в іншому випадку при підготовці приміщення необхідно вимкнути прилади і засоби, що створюють додатковий акустичний фон.

По-друге, в обох випадках слід використати тестові, а що краще всього калібровані, джерела звукового сигналу.

По-третє, в суміжних, по відношенню до того, що перевіряється, приміщеннях має бути забезпечений мінімально можливий рівень акустичного фону.

По-четверте, застосовують практично однакові методи аналізу сигналів («на слух», по осцилограмах і спектрограмах).

Оцінка ефективності віброакустичного захисту приміщення зазвичай проводиться в два етапи. На першому етапі захист, якщо він є, має бути вимкнений і зроблена перевірка власне віброакустичних властивостей поверхонь, що захищають приміщення. Для цього необхідно віброакустичний датчик прикріплювати в різних місцях поверхонь (стіни, дверей, вікон, по можливості підлоги і стелі), що перевіряються, із зовнішньої, по відношенню до контрольованого приміщення, сторони.

Включити джерело тестового звукового сигналу. Воно може розміщуватися або в звичайному місці ведення конфіденційних розмов, або на певній відстані від обстежуваної поверхні (наприклад, як показано на рис. 6).

Рівень звуку зазвичай встановлюють таким, що відповідає гучній мові (74дБ). Для джерел звуку, що калібруються, відстань «L» вибирають в межах 1-2 м. Спочатку на якісному рівні (шляхом прямого прослуховування) оцінюються віброакустичні властивості обстежуваних поверхонь, а потім, переходом в режим «SA», кількісно оцінюються амплітуди частотних складових тестового сигналу.

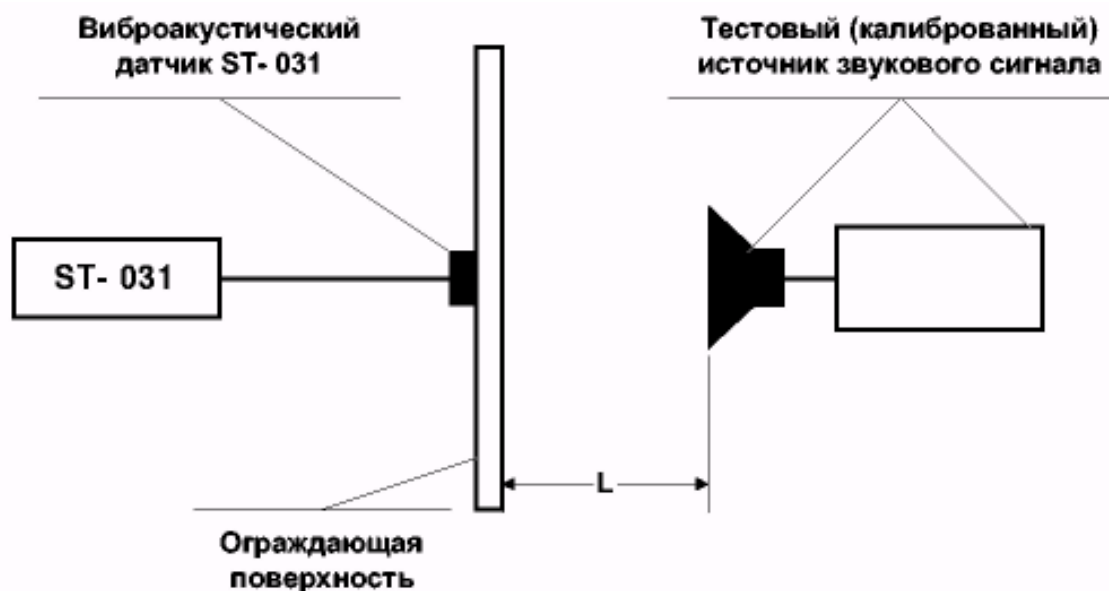


Рис. 6. Схема оцінки віброакустичних властивостей і віброакустичного захисту приміщень

На другому етапі, якщо це передбачено, оцінюється ефективність системи віброакустичного захисту. Для цього на кожній поверхні як якісно «на слух», так і кількісно по спектрограмі визначається співвідношення рівнів тестового і маскуючого сигналу, а також виявляються «не прикриті» складові спектру. Це служить об'єктивною основою корекції амплітудно-частотної характеристики джерел маскуючого сигналу.

Згідно із загальноприйнятими правилами розбірливість мовних сигналів гарантовано не відновлюється, якщо маскуючий шум (перешкода) в 4-5 разів (16 дБ) перевищує їх рівень. Повне виключення ознак мови досягається при 8-ми кратному перевищенні рівня сигналу перешкодою, що створюється системою активного захисту.

Оцінку звукоізоляції приміщень також доцільно проводити в два етапи.

На першому етапі, використовуючи тестове джерело сигналу з рівнем звуку, що відповідає гучній мові, встановити відповідність між цим рівнем і показаннями приладу ST 031 в режимах осцилографа і аналізатора спектру. Для цього розмістити акустичний випромінювач джерела звуку і мікрофон приладу ST 031 на деякій фіксованій відстані. Зазвичай його вибирають у межах 1-2 м (рис. 7).

На другому етапі оцінюються звукоізоляційні властивості поверхонь (стін, дверей, вікон, а якщо можливо, то підлоги і стелі), що захищають

приміщення, ефективність системи активного захисту (зашумлення), а також можливість витoku мовної акустичної інформації через елементи вентиляції, різного роду ніші, наскрізні отвори і т.д.

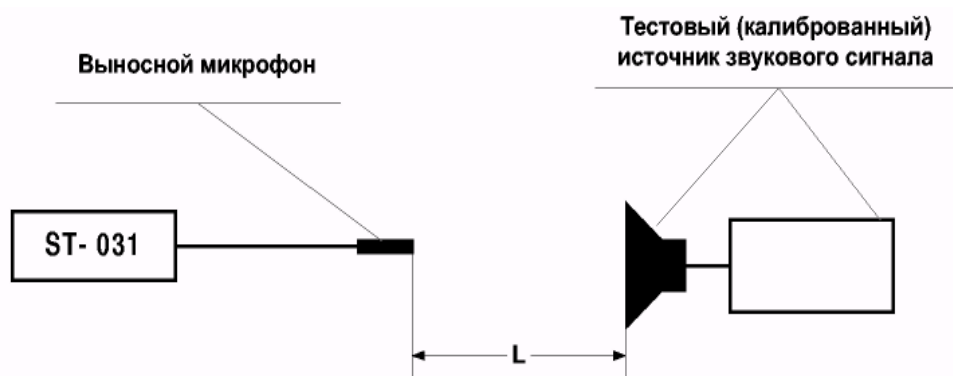


Рис. 7. Схема калібрування індикаторів рівня звукового сигналу приладу ST 031

Для оцінки звукоізоляційних властивостей стін, дверей, підлоги, стелі тестове джерело звуку може бути розташоване або в звичайному місці ведення конфіденційних розмов, або на відстані від обстежуваної поверхні. Наприклад, у варіанті показаному на рис. 8.

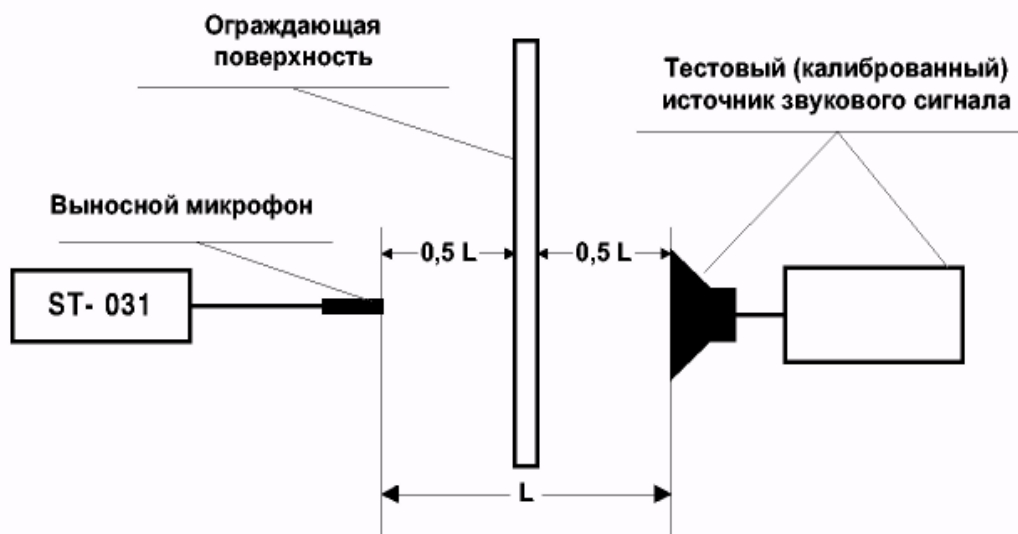


Рис. 8. Схема оцінки звукоізоляції приміщень

Розміщуючи мікрофон в різних місцях суміжних (вище і нижче розташованих) приміщень якісно «на слух» і кількісно по спектрограмі визначити дальність перехоплення мовної інформації з цього приміщення і оцінити зниження рівня звукового сигналу за рахунок властивостей поверхонь, що захищають, а також наявність найменш ослаблених складових спектру. Останнє дає можливість прийняти обґрунтоване рішення про необхідність додаткового захисту, у тому числі і активного і вибір характеристик засобів захисту.

Якщо приміщення розташоване вище за перший поверх, виникають певні труднощі в перевірці звукоізоляції віконних конструкцій. В цьому випадку достатній для якісної оцінки ефект дає наступний, часто використовуваний прийом. Тестове джерело звуку розміщується по будь-якому з раніше розглянутих варіантів. Відкривається квартира, фрамуга або інша частина вікна, залежно від особливостей віконних переплітів. Мікрофон вивішується назовні і в цьому положенні фіксується рівень тестового сигналу, що приймається ним, з приміщення. Потім відкрита частина вікна обережно (щоб не пошкодити кабель мікрофону), але, по можливості, щільно прикривається. Якісно «на слух» і кількісно по осцилограмі або спектрограмі оцінюються звукоізоляційні властивості віконних конструкцій.

Оскільки повітропроводи систем вентиляції прийнято розглядати в якості найбільш небезпечних каналів витоку мовної акустичної інформації, то вони підлягають обов'язковій перевірці. Для цього мікрофон приладу ST 031 необхідно ввести у вихідний (вхідний) отвір повітропроводу кожного з суміжних приміщень, а можливо і деяких інших. Якісно «на слух» оцінити проходження і розбірливість сигналу від тестового джерела, а за свідченнями приладу ST 031 в режимі осцилографа або аналізатора спектру його послаблення при проходженні по повітропроводу до місця розміщення мікрофону. При цьому правильна оцінка послаблення може бути отримана тільки у тому випадку, якщо є детальна схема системи вентиляції. Її наявність дає можливість врахувати послаблення, що вноситься різними елементами конструкції повітропроводів. Так, послаблення мовного сигналу зазвичай складає:

- 0,15 дБ/м - в прямих металевих повітропроводах;
- 0,2 - 0,3 дБ/м - в прямих не металевих повітропроводах;
- 1,0 - 3,0 дБ/м - при зміні перерізу повітропроводу;
- 3,0 - 7,0 дБ/м - на один вигин повітропроводу.

Результати перевірки служать об'єктивною основою для прийняття рішення про необхідність додаткового захисту, для вибору заходів і засобів його забезпечення.

МЕТОДИКА ПОШУКУ ЗАКЛАДНИХ ПРИСТРОЇВ З ВИКОРИСТАННЯМ НЕЛІНІЙНОГО ЛОКАТОРА NR – 900EM



Рис. 1. Зовнішній вигляд нелінійного локатора NR – 900EM

1. Призначення

Нелінійний локатор NR900EM (далі по тексту - виріб) є вимірником вторинних полів і призначений для пошуку пристроїв, що містять напівпровідникові компоненти, незалежно від їх функціонального стану.

Виріб забезпечує можливість ефективного пошуку будь-яких видів радіомікрофонів, у тому числі з дистанційним управлінням, а також мікрофонних підсилювачів дротяних мікрофонів, засобів неявного зйому інформації інфрачервоного і ультразвукового діапазонів, засобів звукозапису. Енергетичний потенціал виробу забезпечує ефективний пошук в елементах інтер'єру і у будівельних конструкціях (підлога, стеля, стіни).

Одновременний прийом другої і третьої гармонік зондуєчого сигналу, візуальна індикація їх рівнів, а також режим виділення огинаючий відбитого сигналу (режим «20К»), дозволяють операторові відрізнити сигнали, відбиті від напівпровідникових радіоелементів від сигналів природних (корозійних) нелінійних відбивачів. Гостронаправлена антенна система, широкий діапазон регулювань основних параметрів виробу забезпечують високу точність локалізації і полегшують проведення пошукових заходів.

2. Технічні дані

Дальність виявлення штатного імітатора (діода 2Д521А) не менше 0,7 м. Живлення виробу здійснюється від вбудованого автономного змінного

джерела - акумулятора «Panasonic VBF – 2E» (час роботи не менше 4 годин.) або від мережі змінного струму 220В, 50 Гц через адаптер мережевого живлення.

Індикація виявлення: візуальна - на чотирьохрядковому моніторі і звукова - на навушники.

Маса виробу в штатній упаковці не перевищує 12 кг. Маса спорядженого блоку приймача не перевищує 3,0 кг.

Середня потужність, що підводиться до антени, не більше 0,1 Вт в режимі «300» і не більше 0,3 Вт в режимі «20К».

Регулювання потужності зондуючого сигналу мінус 8 ± 1 дБ.

Чутливість приймачів при відношенні С/Ш=10дБ не гірше - 115 дБ/Вт.

Динамічний діапазон приймачів не менше 25 дБ.

Регулювання чутливості приймачів здійснюється п'ятьма східцями по мінус 10 ± 2 дБ у кожній.

Коефіцієнти посилення приймальної і передавальної антен не менше 8 дБ.

Поляризація - кругова, коефіцієнт еліпсної не менше 0,75.

Ширина головної пелюстки діаграми спрямованості передавальної і приймальної антен по рівню половинної потужності не більше 40 градусів.

Рівень задніх пелюсток діаграми спрямованості для передавальної і приймальної антен не більше мінус 20 дБ.

3. Склад виробу:

| | |
|---|-------|
| блок приймача | 1 шт. |
| антенна система зі штангою | 1 шт. |
| пульт керування і індикації | 1 шт. |
| комплект ВЧ кабелів | 1 шт. |
| навушники | 1 шт. |
| імітатор | 1 шт. |
| адаптер мережевого живлення | 1 шт. |
| акумулятор | 2 шт. |
| зарядний пристрій | 1 шт. |
| валіза | 1 шт. |
| паспорт | 1 шт. |
| технічний опис та інструкція з експлуатації | 1 шт. |

4. Пристрій і робота

Виріб «NR – 900EM» є портативним приладом, що складається з антенної системи, передавача і двох приймачів, причому приймачі налаштовані на подвійну і потрійну частоту сигналу передавача. Управління режимами роботи здійснюється за допомогою виносного пульта. Зондуючий сигнал передавача перетворюється на нелінійних (напівпровідникових) елементах радіоелектронного пристрою, перевипромінюється, реєструється приймачами і представляється операторові у візуальній і звуковій формі.

5. Конструкція виробу, органи управління і контролю

5.1. Виріб складається з трьох конструктивно незалежних блоків: приймача, антенної системи, а також пульта управління і індикації, що сполучаються між собою кабелями. Антенна система і пульт управління в робочому положенні закріплені на розсувній телескопічній штанзі.

5.2. Блок приймача в робочому положенні за допомогою ременя розташовується на плечі оператора.

На верхній панелі блоку знаходяться роз'єми:

«**OUT**» - вихідний роз'єм передавача, маркований червоною точкою;

«**IN**» - вхідний роз'єм приймача, маркірований синьою точкою;

«**HEADPHONES**» - роз'єм для підключення навушників;

«**AC 15V**» - роз'єм для підключення кабелю адаптера мережевого живлення.

На верхній панелі блоку під кришкою зсуву розташований відсік джерела автономного живлення.

5.3. Органи управління виробом розташовані на пульті управління і виконані у вигляді кнопок, що не фіксуються, забезпечують наступні функції:

ON/OFF - кнопка включення, виключення режиму «**LISTEN MODE**» і виключення живлення виробу;

LIGHT - кнопка включення і виключення фонового підсвічування монітору;

VOLUME (+/-) - Дві кнопки збільшення і зменшення гучності сигналу в навушниках;

300/20 K - кнопка зміни режиму модуляції зондуючого сигналу передавача;

MAX/MIN - кнопка зміни вихідної потужності передавача;

OUT 2/3 - кнопка вибору сигналу, що прослуховується в навушниках, - друга або третя гармоніка;

ATT (+/-) – дві кнопки регулювання чутливості приймачів - збільшення і зменшення послаблення, що вноситься.

5.4. Антенна система виробу розміщується в пластиковому обтічнику. На тильній стороні антенної системи розміщується вузол кріплення її до штанги і два високочастотні роз'єми з кольоровим маркуванням:

- червона точка - передавальна антена, з'єднується кабелем з роз'ємом «**OUT**» на блоці приймача;

- синя точка - приймальна антена, з'єднується кабелем з роз'ємом «**IN**» на блоці приймача.

- синя точка - приймальна антена, з'єднується кабелем з роз'ємом «**IN**» на блоці приймача.

5.5. Зондові антени є відрізками гнучкого провідника завдовжки 0,6 м (2 шт.) і відрізком пружного провідника завдовжки 0,6 м (1 шт.) з роз'ємами на одному з кінців.

5.6. Погоджуючий пристрій, виконаний у вигляді руків'я, на якому розташовані : два роз'єми з кольоровими позначками (червона і синя точки) для підключення до блоку приймача; роз'єм для підключення зондової антени

(без позначки); вузол кріплення пульта управління; вузол кріплення штатної антеної системи.

6. Підготовка до роботи

6.1. Витягнути блоки виробу з штатної упаковки.

6.2. Закріпити антенну систему на штанзі за допомогою вузла кріплення.

6.3. Підключити антенну систему до приймача, дотримуючись кольорового маркування.

Увага. Включення приймача без підключеної антеної системи не допускається.

6.4. Підключити навушники до гнізда «**HEADPHONES**» приймача.

6.5. Встановити акумулятор у відсік, розташований під кришкою зсуву на верхній панелі приймача або підключити роз'єм адаптера мережевого живлення до гнізда DC 15V.

6.6. Підключити кабель пульта управління до роз'єму **CONTROL** приймача. На моніторі повинен відобразитися напис: **RADAR TURNED ON**. Виріб готовий до ввімкнення.

7. Порядок пошуку закладних пристроїв

7.1. Перед включенням виробу переконатися в підключенні антеної системи.

7.2. Одноразово натиснути кнопку **ON/OFF** пульта управління – повинен увімкнутися режим, при якому передавач вимкнений, приймачі включені, атенюатори приймачів встановлені в положення мінус 10 дБ, навушники підключені до виходу приймача другої гармоніки, гучність – в середньому положенні.

За допомогою кнопки **ATT** - встановити максимальну чутливість приймачів, на моніторі в лівій частині 1-го і 2-го рядка повинні відобразитися символи 00. Направляючи антенну систему в різні боки і підключаючи кнопкою **OUT 2/3** навушники до виходів приймачів другої і третьої гармонік, переконатися у відсутності перешкод на частотах прийому при максимальній чутливості приймачів. Інакше оцінити можливість роботи з виробом, встановивши атенюатори приймачів так, щоб сигнал перешкоди виявився нижче порогу чутливості.

7.3. Повторно натиснути кнопку **ON/OFF** пульта управління – повинен увімкнутися режим «300», вихідна потужність передавача – максимальна, атенюатори приймачів і навушники знаходяться в положенні, вибраному в п. 7.2.

Примітка. Третє натиснення кнопки **ON/OFF** - виключення виробу, при цьому на екрані відображається напис: **RADAR TURNED OFF**.

При відключенні виробу кнопкою **ON/OFF** «положення» органів управління виробу, встановлене оператором, запам'ятовується і при повторному включенні відновлюється. При відключенні або заміні акумулятора режими роботи виробу після включення встановлюються, як описано в п. 7.2.

Вид інформації, що відображається на дисплеї, представлений на рис. 2.

У першому і другому рядках відображається рівень послаблення атенюаторів приймачів, відносний рівень сигналів другої і третьої гармонік в псевдоаналоговому і цифровому вигляді і в одному з цих рядків -значок П, який вказує, до якого приймача виробу підключені навушники. Перемикання навушників здійснюється кнопкою **OUT 2/3**, при цьому значок переміщається з одного рядка в інший. У третьому рядку відображається різниця рівнів другої і третьої гармонік. Знак «-» означає, що третя гармоніка перевищує другу.

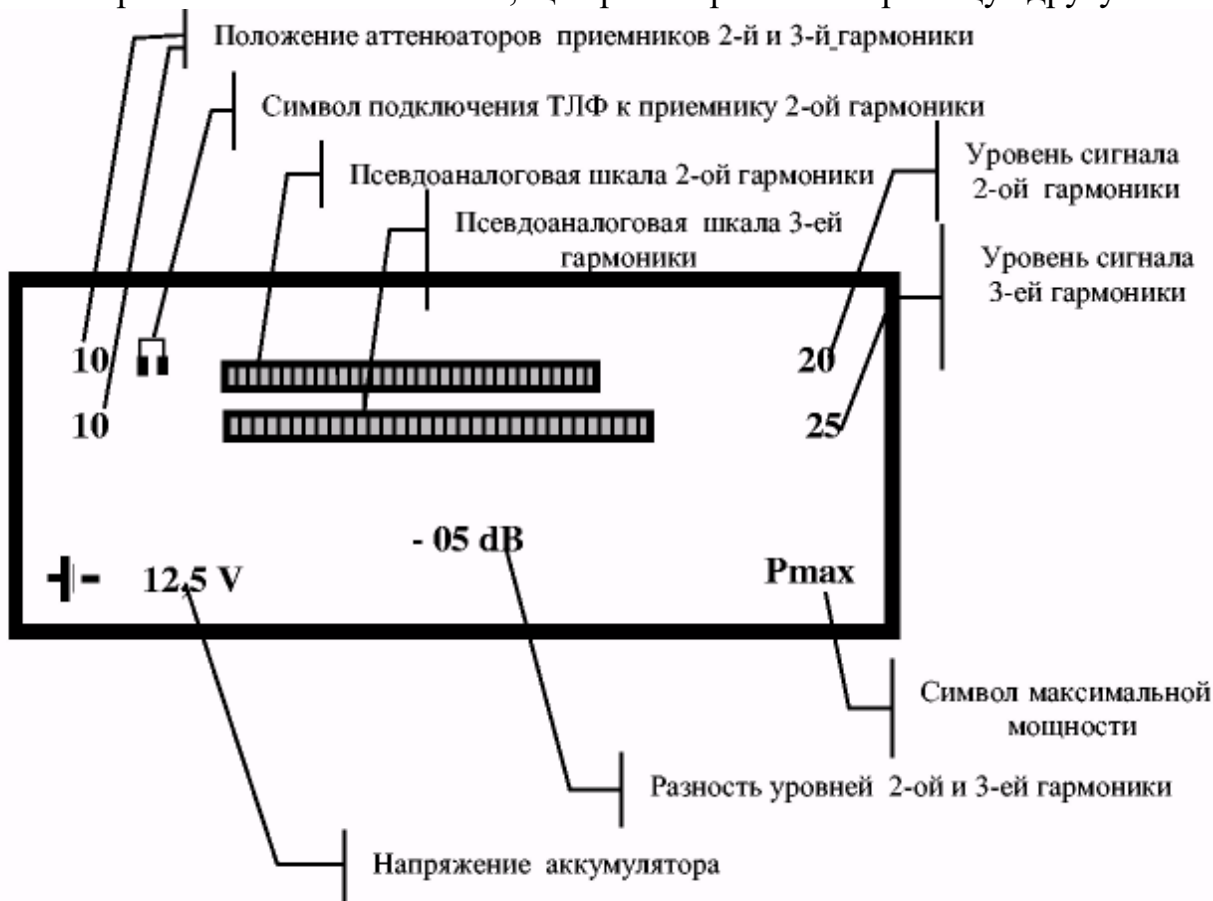


Рис. 2. Вид інформації, що відображається, на дисплеї

У разі перевантаження приймачів в цьому рядку з'являється напис «**OVER**».

У лівій частині четвертого рядка відображається напруга акумулятора, а в правій - відносний рівень вихідної потужності передавача у вигляді символів **Pmax** або **Pmin**. Зміна потужності здійснюється кнопкою **MAX/MIN**.

У разі розряду акумулятора нижче рівня напруги 11,1 В, в четвертому рядку з'явиться напис: «**CHANGE BATTERY**», а в навушниках - переривчастий звуковий сигнал.

Увага. Зберігання розряджених акумуляторів не допускається.

7.4. За допомогою штатного імітатора переконатися в працездатності виробу. Для цього розташувати імітатор у вільному місці за відсутності поблизу радіоелектронної апаратури. Встановити максимальний рівень зондуємого сигналу за допомогою кнопки **MAX/MIN** (на дисплеї в правій частині 4-го

рядка повинен відображатися символ P_{max}) і максимальну чутливість за допомогою кнопок **ATT** (на дисплеї в лівій частині 1-го і 2-го рядка повинні відображатися символи 00). За допомогою кнопки **OUT 2/3** перемкнути навушники на вихід приймача 2-ої гармоніки. Направити антенну систему у бік імітатора з відстані 0,7-0,8 м. У навушниках повинен прослуховуватися тональний сигнал частотою 300 Гц середньої гучності, а на моніторі в 1-му і 2-му рядку повинен відображатися рівень сигналу 2-ої, що приймається, і 3-ї гармоніки відповідно, причому рівень, що відображається в правій частині, має бути не меншим 10-15 і 5-10 дБ відповідно, а різниця рівнів, що відображається в 3-му рядку, повинна бути не менше 5 дБ. Видалення імітатора із зони зондування при незмінному положенні антенної системи повинне призводити до зникнення сигналу-відгуку.

7.5. Провести пошук напівпровідникових елементів, працюючи залежно від обстановки перешкод, по можливості, з максимальною потужністю і максимально можливою чутливістю. Для цього переміщати антенну систему уздовж обстежуваної поверхні. При появі в навушниках тонального сигналу частотою 300 Гц грубо визначити місце розташування перевідбиваючого об'єкту. У міру наближення до нього антенної системи інтенсивність тону в навушниках посилюватиметься.

7.6. Стежити за співвідношенням сигналів-відгуків 2-ої і 3 - ї гармонік на дисплеї. У разі істотного перевищення рівня сигналу 3-ї гармоніки над 2-ою найімовірніше, що джерелом сигналу-відгуку є корозійна нелінійність. Для достовірної ідентифікації відгуку, не міняючи орієнтацію і місце розташування антенної системи, перевести аналізатор в режим «20К». Для цього натиснути кнопку **300/20К**.

7.7. Встановити максимальну потужність передавача, максимальну чутливість приймачів і максимальну гучність сигналу в навушниках. Переконатися в тому, що прослуховуються модуляційні сигнали другої гармоніки зондуемого сигналу.

7.8. Максимально наблизити антенну систему до обстежуваної поверхні в точці виявлення перевідбиваючого об'єкту. Переміщати антену паралельно обстежуваній поверхні від точки виявлення до периферії на 30-40 см і назад, стежити за рівнем шумового сигналу в навушниках.

7.9. Залежно від характеру перевідбиваючого об'єкту - корозійний діод або штучний напівпровідниковий елемент (радіоелектронний пристрій), можливі дві принципово різні залежності рівня шуму в навушниках від переміщення антенної системи уздовж обстежуваної поверхні. Їх типовий вид представлений на рис. 3, 4.

7.10. Для підвищення достовірності рекомендується прослухати шумовий відгук в навушниках аналізатора в режимі «20К» при простукуванні місця розташування відбиваючого об'єкту яким-небудь неметалічним предметом.

При цьому корозійний діод, як правило, характеризується хрипким нерегулярним хрускотом.

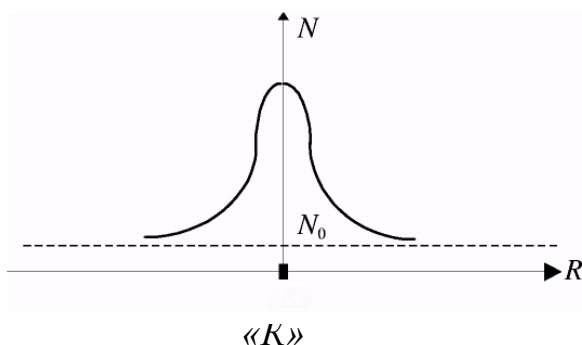


Рис. 3. Залежність рівня модуляційних шумів 2-ої гармоніки корозійного рп- переходу від відстані від об'єкту до осі антенної системи аналізатора.

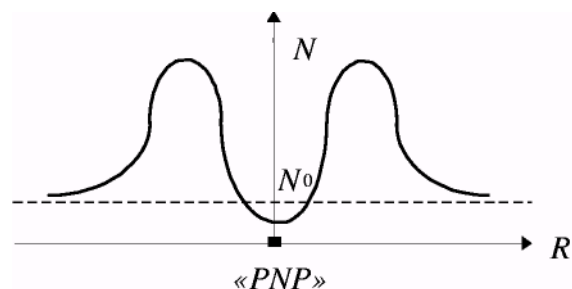


Рис. 4. Залежність рівня модуляційних шумів 2-ої гармоніки напівпровідникового рп- переходу від відстані від об'єкту до осі антенної системи аналізатора.

На рис. 3, 4 позначені:

«К» - точка розташування корозійного рп- переходу;

«PNP» - точка розташування напівпровідникового елемента;

N - рівень шуму в навушниках;

N_0 - рівень шуму в навушниках за відсутності нелінійного перевідбиваючого об'єкту;

R - відстань від точки розташування перевідбиваючого об'єкту до осі антенної системи виробу.

7.11. При переході в режим прослуховування модуляції 3-ї гармоніки зонduючого сигналу залежності шумів в навушниках протилежні (криві, зображені на рис. 2 і 3, міняються місцями).

7.12. Істотне перевищення 2-ї гармоніки зонduючого сигналу над 3-ю гармонікою (20 дБ і більше) з високою мірою вірогідності свідчить про штучний характер перевідбиваючого об'єкту.

7.13. Після роботи вимкнути виріб, роз'єднати його блоки і скласти в штатну укладку. Рекомендований порядок роз'єднання:

- витягнути акумулятор з відсіку живлення корпусу приймача;
- відключити роз'єм пульта управління;
- відключити коаксіальні кабелі від антенної системи і блоку приймача.

8. Вказівки по техніці безпеки

8.1. Середня потужність, що підводиться до антени виробу в режимі «300» не перевищує 100 мВт, в режимі «20К» - 300 мВт, що приблизно в 4-10 разів менше потужності мобільного телефону.

8.2. Щільність потоку потужності зонduючого сигналу аналізатора у напрямі максимального випромінювання на відстані 1 м не перевищує норм, встановлених ДСТУ 12.1.006-84 для 8 годин безперервної роботи персоналу, обслуговуючого НВЧ установки.

Проте, при використанні виробу слід дотримуватися правил техніки безпеки, прийнятих при роботі з приладами, що мають відкриті випромінювачі радіочастотної енергії:

- не направляти антенну систему у бік очей при відстані між антенним блоком і людиною менш одного метра;
- уникати тривалого перебування людей в зоні головної пелюстки діаграми спрямованості антенної системи.

МЕТОДИКА ПОШУКУ ЗАКЛАДНИХ ПРИСТРОЇВ З ВИКОРИСТАННЯМ ІНДИКАТОРА ПОЛЯ PROTECT 1203



Рис. 1. Загальний вигляд індикатора поля PROTECT 1203

1. Призначення

Індикатор електромагнітного поля PROTECT 1203 призначений для пошуку і виявлення облаштувань НСІ, коли вони знаходяться в активному режимі і використовують як канал передачі інформації електромагнітні випромінювання. За допомогою PROTECT 1203 можна перевіряти приміщення, машини, різні предмети, а також людей на предмет наявності переносних передавачів. Пошук може здійснюватися в прихованому режимі, для чого використовується вбудований в прилад вібратор. Індикатор також визначає наявність у співрозмовника працюючого мобільного телефону.

2. Загальні відомості

2.1. Перед початком проведення пошуку необхідно висунути антену, включити живлення і поза зоною перевірки встановити необхідний рівень чутливості. Потім в приміщенні, де здійснюється перевірка, методично обстежуються усі кімнати, при цьому наявність засобів НСІ визначається світловою індикацією. Якщо немає можливості постійно стежити за індикатором, то можна орієнтуватися на вбудований в прилад вібратор.

2.2. Корпус PROTECT 1203 виконаний з міцного дюралюмінієвого сплаву, який захищає пристрій від ударних ушкоджень і підвищеної вологості,

проте не рекомендується зберігати і використовувати індикатор в поганих умовах.

2.3. Живлення PROTECT 1203 здійснюється від 2 батарей або акумуляторів формату AAA. Алкалайнові батареї забезпечують безперервну роботу протягом 10 годин. Після розрядки джерел живлення можна зарядити акумулятори або замінити батареї.

2.4. Зовнішній вигляд приладу. На передній панелі приладу (рис.1) розташовані органи управління для включення-виключення живлення, регулювання рівня чутливості і індикатор відображення відносного рівня радіополя. У нижній частині приладу знаходиться відсік для батарей. Висувна антена на задній панелі приладу служить для прийому радіосигналів. Для нормальної роботи PROTECT 1203 необхідно висувати як мінімум перший (найширший) сегмент антени.

Органи управління і індикації.

POWER - блакитний світлодіод на лівій стороні передньої панелі відображає режим, в якому знаходиться прилад (включений/вимкнений). Кнопка праворуч від світлодіода служить для включення/виключення приладу.

SENS - регулятор чутливості приладу. Для відображення рівня чутливості і рівня РП служить світлова індикація зліва від регулятора.

3. Керівництво по проведенню пошукових заходів

3.1. Підготовка до пошуку

При підготовці до пошуку необхідно, відповідно до плану (додаток 1), провести заходи по активізації впроваджених закладних пристроїв, що включаються дистанційно або за принципом акустопуска. В якості цих заходів може бути:

- організація «неправдивої» зустрічі або переговорів;
- відтворення на магнітофоні доповідей, записаних на відкритій нараді;
- програвання музичних композицій та ін.

Пошук бажано здійснювати в робочий час. Окрім вищеперелічених заходів необхідно закрити усі вікна і штори в приміщенні. Включити освітлення і офісне приладдя для створення звичайних умов роботи. Перш ніж входити в приміщення, що перевіряється, необхідно включити прилад і висунути антену на середню довжину. Необхідно переконатися, що висунений перший (найширший) сегмент антени. Це важливо! Можна сховати інші сегменти антени, але перший сегмент має бути висунений.

Налаштування чутливості приладу. Для цього ручка налаштування обертається до тих пір, поки не світлитиметься або не блиматиме тільки один сегмент на світлоіндикаторі. Якщо під час пошуку оператор не хоче, або не має можливості спостерігати рівень РП за допомогою світлоіндикатора, то можна встановити чутливість, при якій горять усі зелені сегменти. В цьому випадку при наближенні до джерела випромінювання, спалахнуть червоні сегменти, і включитися вбудований вібратор.

3.2. Пошук ЗП в приміщеннях

1) Увійдіть до приміщення, що перевіряється, тримаючи PROTECT 1203 вертикально і спостерігаючи світіння світлоіндикатора. Включіть і вимкніть світло, офісне приладдя і інші електроприлади. Спостерігайте зміни показань приладу. Якщо вони міняються синхронно з включенням/виключенням якогось приладдя, то це сигнал про можливу наявність в цьому приладі облаштування несанкціонованого знімання інформації.

2) Обійдіть усю кімнату, спостерігаючи показання приладу. При наближенні/видаленні до джерела випромінювання відповідно збільшуватиметься/зменшуватися показуваний рівень випромінювання.

3) Визначите місця з найбільшим рівнем випромінювання переміщаючи прилад у всіляких напрямках і спостерігаючи світіння світлоіндикатора.

4) Перевірте усі об'єкти, які можуть містити приховані облаштування неявного знімання інформації. Сигналом про виявлення подібного роду передавачів є знову-таки зміни свідчень світлового індикатора.

5) Намагайтеся точно визначити місцезнаходження джерела нелегального випромінювання. Для цього зменшіть до мінімуму чутливість приладу. Якщо антена висунена не повністю, то рівень РП, що відображається на світловому індикаторі, не залежатиме від взаємного розташування антени і передавача, і ви спостерігатимете постійний рівень випромінювання поблизу передавача. Іноді світлоіндикатор може показати збільшення рівня РП поблизу дротів або металевих об'єктів. Це пов'язано з тим, що металеві об'єкти виступають як «продовження» антени і такі ситуації не обов'язково сигналізують про наявність передавача.

6) Після визначення точного місцезнаходження джерела випромінювання приступайте до фізичного пошуку. Зробіть візуальний огляд і перевірте за допомогою PROTECT 1203 всі об'єкти, що знаходяться в «небезпечній» зоні. Розберіть, якщо це можливо, освітлювальні прилади, телефони, розетки живлення, телефонні розетки і тому подібне. Дуже ретельно оглянете телефонні лінії і лінії 220 В. Прогляньте усі книги, вміст столів і тому подібне.

7) Якщо оператор виявив облаштування знімання інформації - не припиняйте подальший пошук! Ви повинні максимально уважно продовжувати пошук, оскільки немає ніякої гарантії, що вас підслуховували тільки за допомогою одного передавача. Професіонали часто «ставлять» 2 облаштування прослуховування - одне досить легко визначуване, а друге добре замасковане, з дистанційним управлінням, з нестандартною модуляцією і тому подібне.

3.3. Перевірка телефонних ліній

Телефонний ЗП може бути встановлено на будь-якому відрізку телефонної лінії. Він може бути встановлений в телефонному апараті, телефонній розетці, комутаційній коробці або на телефонному кабелі. Більшість телефонних ЗП активізується тільки при піднятті трубки, тому перевірка виконується при піднятій трубці.

Розпочніть перевірку з телефонного апарату. Розмістіть антену PROTECT 1203 біля апарату і підніміть трубку. Спостерігайте зміни рівня радіополя.

Якщо ви перевіряєте радіотелефон, то, природньо, виявите сильне збільшення рівня радіополя при знятті трубки з бази, пов'язане з тим, що трубка і база зв'язуються по радіоканалу. Але особливого сенсу перевіряти радіотелефон немає. Радіотелефон сам по собі є прекрасним радіопередавальним пристроєм.

Переміщайте антену приладу уздовж телефонної лінії при піднятій трубці. Перевірте усі розетки і комутаційні коробки. Якщо у Вас є асистент, то попросіть його кілька разів підняти і покласти трубку. Якщо Ви помітите, що рівень радіополя змінюється синхронно з підняттям/опусканням трубки, то це сигнал про наявність на лінії жучка. Спробуйте визначити ділянку лінії з максимальним рівнем випромінювання і проведіть ретельний фізичний пошук.

3.4. Перевірка людей

Існує велика кількість передавачів, що вбудовуються в одяг, особисті речі відвідувача і тому подібне. Ці пристрої можуть транслювати переговори або (і) відеоінформацію. Для перевірки необхідно налаштувати чутливість так, щоб світилися усі зелені сегменти світлоіндикатора. З метою маскування перевірки, сховайте PROTECT 1203 в кишені або під одягом, заздалегідь висунувши перший (найширший) сегмент антени і включіть живлення приладу. Наблизьтеся до людини, що перевіряється. Включення вібратора сигналізує про наявність радіопередавального пристрою.

Інший метод перевірки - це розташування PROTECT 1203 під столом з висунутою антеною по можливості ближче до співрозмовника. Спостерігайте зміни свідчень світлоіндикатора, коли підозріла персона сідає за стіл або встає з-за столу.

4. Дальність виявлення

Дальність виявлення нелегальних облаштувань знімання інформації залежить від двох важливих чинників:

1. Вихідної потужності закладного пристрою.
2. Радіообстановки в приміщенні - рівня випромінювання ТБ, радіостанцій і легальних засобів комунікації.

Рівень, що відображається на світлоіндикаторі PROTECT - 1203 збільшується при наближенні до джерела радіовипромінювання. Збільшення рівня може викликати не лише нелегальний пристрій, але і безпечні сигнали ТБ або радіо.

Локалізація місцезнаходження нелегального передавача зводиться до знаходження області, де спостерігається максимальний рівень випромінювання. Безпосереднє виявлення ЗП здійснюється фізичним пошуком закладних пристроїв.

**ВАРІАНТ АКТУ КОМПЛЕКСНОЇ
СПЕЦІАЛЬНОЇ ПЕРЕВІРКИ ПРИМІЩЕНЬ**

Екз. №
Усього екз.

**АКТ
комплексної спеціальної перевірки приміщення
на наявність засобів неявного знімання інформації
за договором № ___ від _____ 20__ р.**

Ми, що підписалися нижче, представник Замовника, в особі Генерального директора (назва підприємства, прізвище, ініціали) _____, з одного боку, і представник Підрядника, в особі Генерального директора ТОВ "Агентство _____" _____, з іншого боку, склали цей Акт про те, що роботи за договором № ___ від _____ 20__ року виконані в повному об'ємі і задовольняють вимогам договору.

1. У період з _____ по _____ на підприємстві (найменування підприємства) проведена комплексна спеціальна перевірка приміщень, в яких циркулює конфіденційна інформація, на наявність закладних пристроїв і інших засобів неявного знімання інформації. Роботи виконувалися на підставі виданої ТОВ "Агентство _____" Ліцензії ДССЗ і ЗІ № _____ від _____ 20__ р.

2. Склад пошукової бригади:

- 1) _____ - керівник;
- 2) _____;
- 3) _____.

3. Перевірені наступні приміщення:

- 1) Кабінет керівника підприємства.
- 2) Приміщення бухгалтерії.

4. В ході перевірки проведені наступні роботи:

- 1) Візуальний огляд конструкцій, що захищають, меблів і інших предметів інтер'єру (трудовитрати - __ люд. годин).
- 2) Перевірка елементів будівельних конструкцій, меблів і інших предметів інтер'єру з використанням спеціальних пошукових технічних засобів (__ люд. годин).
- 3) Перевірка ліній і устаткування силової і освітлювальної електромережі (__ люд. годин).
- 4) Перевірка ліній і устаткування абонентської телефонної мережі (__ люд. годин).
- 5) Перевірка ліній і устаткування пожежної і охоронної сигналізації (__ люд. годин).

- 6) Перевірка радіоефіру на присутність сигналів радіовипромінюючих засобів неявного знімання інформації (радіомоніторинг приміщення) (__ люд. годин).
- 7) Перевірка несанкціонованих передач інформації в діапазоні інфрачервоного випромінювання (__ люд. годин).
- 8) Пошук закладних пристроїв, що використовують низькочастотні магнітні випромінювання (__ люд. годин).
- 9) Пошук пасивних закладних пристроїв (__ люд. годин).
- 10) Дослідження приміщення на предмет наявності акустичного і віброакустичного каналів витоку інформації (__ люд. годин).
- 11) Фізичний пошук закладних пристроїв і інших засобів НОІ (__ люд. годин).

5. В ході перевірки використовувалася наступна пошукова і дослідницька апаратура:

- 1) Пошуковий програмно-апаратний комплекс ПАК DigiScan, що складається з портативного комп'ютера Toshiba (зав. № __) зі спеціальним ПЗ DigiScan 2000 скануючого приймача AR – 3000A (зав. № __).
- 2) Багатофункціональний пошуковий прилад ST 031 «Піранья» (зав. № __).
- 3) Нелінійний локатор NR900EM (зав. № __).
- 4) Портативний частотомір RFM - 32 (зав. № __).
- 5) Індикатор електромагнітного поля PROTECT - 1203 (зав. № __).

6. Результати перевірки:

1) В кабінеті керівника виявлений підслуховуючий пристрій з передачею перехоплюваної акустичної інформації по дротах силової електричної мережі. Пристрій на момент перевірки працездатний, виконаний у вигляді трійника-розгалужувача і підключений до розетки електричної мережі біля робочого столу керівника підприємства. Радіус знімання акустичної інформації - близько шести метрів, дальність передачі перехоплюваної інформації - до силового трансформатора, розміщеного в електросиловій будці, що знаходиться за межами території, що охороняється.

Найбільш вірогідні місця знімання передаваної інформації: електророзетки в приймальні, коридорі, підсобних приміщеннях і туалетній кімнаті, електросиловий щит на сходовому майданчику, електросилова будка за межами підприємства.

Вірогідний час установки - (дата), під час проведення ремонту кабінету.

Виявлений підслуховуючий пристрій нейтралізований шляхом акустичної ізоляції мікрофону і залишений на місці виявлення.

Інших засобів неявного знімання інформації в кабінеті керівника не виявлено.

2) В приміщенні бухгалтерії засобів неявного знімання інформації не виявлено.

3) Кабінет керівника підприємства недостатньо захищений від витоку інформації, що захищається, по технічних каналах:

- можливий витік акустичної інформації через канал природної вентиляції приміщення;

- можливий витік акустичної інформації через віброакустичний канал, утворений магістраллю парового опалювання;

- можливе несанкціоноване знімання інформації з монітора комп'ютера шляхом перехоплення його побічних електромагнітних випромінювань.

Приміщення бухгалтерії не захищене від витоку інформації, що захищається, по технічних каналах:

- можливий витік акустичної інформації через тонкі двері і гіпсокартонну частину перегородки з приміщенням приймальні;

- можливий витік акустичної інформації через канал природної вентиляції приміщення;

- можливий витік акустичної інформації через віброакустичний канал, утворений магістраллю парового опалювання;

- існує можливість дистанційного, без підключення додаткових облаштувань перехоплення телефонних переговорів, що ведуться з радіотелефону PANASONIC;

- можливе несанкціоноване знімання інформації з моніторів комп'ютерів і іншої оргтехніки шляхом перехоплення побічних електромагнітних випромінювань;

- можливий витік інформації, що знімається візуально або з використанням фото- і відеотехніки, через незашторене вікно і зашклену частину вхідних дверей.

Перевірені приміщення не захищені від несанкціонованого запису конфіденційних переговорів на диктофон, зйомки прихованими відеокамерами і можливого витоку інформації за рахунок наведень в провідних лініях, прокладених паралельно дротам телефонної мережі. Приміщення мають багато місць, зручних для встановлення радіомікрофонів або швидкої установки інших видів засобів неявного знімання інформації.

7. Рекомендації по підвищенню захищеності перевірених приміщень і відвертанню витоку інформації по виявлених технічних каналах її витоку викладені в окремому документі.

8. Договірна ціна складає _____ (_____) грн, у тому числі ПДВ 20% _____ (_____) грн.

Взаєморозрахунки зроблені повністю. Сторони не мають претензій один до одного.

Роботу здав:

Генеральний директор ТОВ

«Агентство _____»

« _____ » _____ 20 _ р.

Роботу прийняв:

Генеральний директор

« _____ » _____ 20 _ р.

**ВАРІАНТ РЕКОМЕНДАЦІЙ
ПО ПІДВИЩЕННЮ ЗАХИЩЕНОСТІ
ПЕРЕВІРЕНИХ ПРИМІЩЕНЬ І ОБ'ЄКТІВ**

Екз. №_

Усього_екз.

**РЕКОМЕНДАЦІЇ
по підвищенню захищеності
перевірених приміщень _____**

1. Перелік виявлених в перевірених приміщеннях потенційних технічних каналів витоку інформації (ТКВІ):

1. Кабінет керівника підприємства:

- 1) акустичний повітряний ТКВІ через канал природної вентиляції приміщення;
- 2) акустичний вібраційний ТКВІ через канал природної вентиляції приміщення;
- 3) акустичний вібраційний ТКВІ через магістраль (трубопровід) парового опалювання приміщення;
- 4) електромагнітний ТКВІ за рахунок перехоплення ПЕМІ монітора комп'ютера;
- 5) електричні ТКВІ за рахунок знімання наведень з дротяних ліній пожежної і охоронної сигналізації, прокладених паралельно дротам телефонної лінії.

2. Приміщення бухгалтерії:

- 1) акустичний повітряний ТКВІ через канал природної вентиляції приміщення;
- 2) акустичний повітряний ТКВІ через входні двері приміщення;
- 3) акустичний повітряний ТКВІ через гіпсокартонну перегородку з приміщенням приймальні;
- 4) акустичний вібраційний ТКВІ через канал природної вентиляції приміщення;
- 5) акустичний вібраційний ТКВІ через гіпсокартонну перегородку з приміщенням приймальні;
- 6) акустичний вібраційний ТКВІ через магістраль (трубопровід) парового опалювання приміщення;
- 7) електромагнітні ТКВІ за рахунок перехоплення ПЕМІ моніторів комп'ютерів і іншої оргтехніки;
- 8) електричні ТКВІ за рахунок знімання наведень з дротяних ліній

пожежної і охоронної сигналізації, прокладених паралельно дротам телефонної лінії;

9) можливий витік інформації за рахунок прямого перехоплення сигналів радіотелефону PANASONIC;

10) можливий витік інформації, що знімається візуально або з використанням фото- і відеотехніки, через незашторене вікно і зашклену частину вхідних дверей.

Обидва приміщення не захищені від несанкціонованого запису на диктофон, зйомки прихованими відеокамерами і підкиду радіомікрофонів. Схеми виявлених потенційних ТКВІ з короткими поясненнями – у додатку до документа.

2. Оцінка вірогідності використання супротивником потенційних ТКВІ і захищеності приміщень:

1. Кабінет керівника підприємства :

Зважаючи на хорошу чутність і розбірливість мовних сигналів і доступність для відвідувань сусідніх приміщень вірогідність використання акустичного повітряного і акустичного вібраційного потенційних ТКВІ можна вважати високою.

Використання акустичного вібраційного ТКВІ через магістраль (трубопровід) парового опалювання, через слабку розбірливість сигналів можна вважати вірогідним.

Використання електромагнітного ТКВІ за рахунок перехоплення ПЕМІ монітора комп'ютера і електричного ТКВІ за рахунок знімання наведень з дротяних ліній можна вважати маловірогідним, але можливим.

У зв'язку з відсутністю в кабінеті спеціальних засобів захисту інформації від витоку по виявлених потенційних ТКВІ, а також високою вірогідністю використання супротивником акустичного повітряного і акустичного вібраційного потенційних ТКВІ, кабінет керівника підприємства слід вважати незахищеним від витоку інформації, що захищається, по технічних каналах.

2. Приміщення бухгалтерії:

(далі дається оцінка вірогідності використання потенційних ТКВІ і оцінка захищеності приміщення від неявного знімання інформації).

3. Рекомендації по заходах і способах відвертання знімання інформації по виявлених потенційних ТКВІ і підвищенню захищеності приміщень:

1. Кабінет керівника підприємства:

1) Для захисту приміщення від витоку акустичної інформації через канал природної вентиляції приміщення рекомендується зашумлення каналу шляхом створення акустичних і вібраційних перешкод за допомогою генератора акустичного шуму. Найбільш ефективною системою захисту є

комплекс віброакустичного захисту БАРОН. Частковою, дешевшою альтернативою комплексу можна рахувати генератор акустичного шуму ANG - 2000. Ці ж засоби забезпечать захист приміщення від витоку акустичної інформації через магістраль (трубопровід) парового опалювання і захищаючі кабінет будівельні конструкції.

2) Для захисту приміщення від витоку інформації за рахунок перехоплення ПЕМІ монітора комп'ютера рекомендується електромагнітне зашумлення приміщення за допомогою генератора шуму ГРІМ-ЗІ-4. Застосування цього генератора забезпечить також створення перешкод засобам несанкціонованого знімання інформації з електричної мережі, що запобіжить витоку інформації у разі повторного використання супротивником підслуховуючого пристрою, аналогічного знайденому в ході перевірки. В якості альтернативи генератору шуму ГРІМ-ЗІ-4 по електромагнітному зашумленню приміщення може розглядатися генератор шуму ГРІМ-3 або ГШ-К-1000.

3) Для відвертання витоку інформації за рахунок знімання наведень з дротяних ліній пожежної і охоронної сигналізації рекомендується перепрокладка телефонної лінії для усунення її спільного паралельного пробігу з лініями пожежної і охоронної сигналізації. Альтернативою перепрокладки телефонної лінії є установка в лініях пожежної і охоронної сигналізації перешкодопригнічуючих фільтрів ФП-7.

4) Для захисту приміщення від несанкціонованого аудіозапису рекомендується застосування пригнічувача радіоелектронних облаштувань неявного аудіозапису ШТОРМ.

5) Для своєчасного виявлення несанкціонованої відеозйомки рекомендується установка в кабінеті індикатора прихованих відеокамер Iris VSF - 2000.

2. Приміщення бухгалтерії:

Для захисту приміщення від витоку акустичної інформації... (далі даються рекомендації номерам і способам відвертання знімання інформації по виявлених ТКВІ і підвищенню захищеності приміщення бухгалтерії).

4. Звідний перелік технічних засобів і систем захисту інформації, рекомендованих для підвищення захищеності приміщень.

Для захисту вищезгаданих приміщень рекомендується застосування наступного устаткування і приладдя (таблиця. 1).

Рекомендоване обладнання і системи захисту

Таблиця 1

| Приміщення | № п/п | Рекомендовані засоби | Альтернативні засоби | Призначення | Необхідна кількість |
|--------------------------------|-------|---|---|--|---------------------|
| Кабінет керівника підприємства | 1 | Комплекс віброакустичного захисту DNG-2300 | Генератор акустичного шуму ANG - 2000 | Захист приміщень від витоку акустичної інформації через канали природної вентиляції, трубопровід опалювання, що захищають будівельні конструкції | 1 |
| | 2 | Захисний пристрій БАЗАЛЬТ - 5ГЕШ | | Захист від ПЕМІ | 2 |
| | 3 | Пристрій забезпечення конфіденційних переговорів пригнічувач диктофонів DRUID D-06 | | Захист приміщень від несанкціонованого запису на диктофон | 1 |
| | 4 | Пристрій для пошуку прихованих відеокамер WEGAi | | Своєчасне виявлення несанкціонованої відеозйомки в приміщенні | 1 |
| Приміщення бухгалтерії | 6 | Далі наводиться перелік технічних засобів і систем захисту інформації, рекомендованих для підвищення захищеності приміщення бухгалтерії | | | |
| | 7 | | | | |
| | 8 | | | | |
| | 9 | | | | |
| | 10 | | | | |
| | 11 | | | | |
| Приміщення служби безпеки | 12 | Пошуковий комплекс Delta X 100/4 для пошуку підслуховуючих пристроїв | Аналізатор спектру OSCOR Green (OGR-24) | Устаткування пункту радіоконтролю для постійного радіомоніторингу службових приміщень | 1 |
| | 13 | Багатоканальний цифровий магнітофон | | Забезпечення гласного контролю акустики службових приміщень і встановлених керівництвом обмежень на використання каналів зв'язку | 1 |
| | 14 | | | | |

5. Пропозиції по практичному використанню рекомендованих засобів і систем захисту інформації:

1. Комплекс віброакустичного захисту здатний забезпечити одночасний захист усіх перевірених приміщень.

У кабінеті керівника підприємства доцільно встановити один пристрій контролю ефективності вібраційних перешкод і шість віброгенераторів типу: по одному в кожному вентиляційному каналі, по одному на скло вікна, на трубопровід парового опалювання, балку стельового перекриття і на плиту перекриття між другим і третім поверхами.

У приміщенні бухгалтерії доцільно встановити чотири віброгенератори і один пристрій контролю ефективності вібраційних перешкод. Рекомендовані місця установки відображені на схемі (додатки №.)

Установку основного блоку (генератора) комплексу віброакустичного захисту і пристроями дистанційного включення віброгенераторів рекомендується провести в приміщенні служби безпеки.

Включення перешкодного сигналу в приміщеннях, що захищаються, рекомендується здійснювати з приміщення служби безпеки на час ведення конфіденційних переговорів. Контроль ефективності перешкод доцільно здійснювати по сигналу тривоги, що подається пристроями, встановленими в приміщеннях, що захищаються.

2. Генератори шуму рекомендується встановити по одному в кожному приміщенні, що захищається.

Включення електромагнітного зашумлення приміщення в кабінеті керівника підприємства доцільно здійснювати на час роботи з ПЕВМ, в приміщенні бухгалтерії - з початком робочого дня.

Включення режиму лінійного зашумлення електромережі рекомендується з початком робочого дня, виключення - після його закінчення.

Режим захисту телефонної лінії генератором шуму в кабінеті керівника підприємства використовувати не рекомендується у зв'язку із застосуванням для цієї мети ефективнішого пристрою захисту ПРОКРУСТ-2000.

3. Установку перешкодоподавляючих фільтрів ФП-7 в лінії пожежної і охоронної сигналізації приміщень, що захищаються, рекомендується здійснити згідно з схемами додатки №.

4. Пригнічувач радіоелектронних пристроїв неявного аудіозапису рекомендується включати за допомогою пульта дистанційного керування на час проведення нарад і конфіденційних переговорів.

5. (далі тривають пропозиції по практичному використанню засобів і систем захисту інформації, рекомендованих для підвищення захищеності приміщень).

Додатки (не додаються):

1. Схеми виявлених за результатами перевірки потенційних технічних каналів витоку інформації.

2. Схеми установки рекомендованих засобів систем захисту інформації.

Погоджено

Керівник організації що
проводить перевірку

_____/_____/

" ____ " _____ 20__ г.

**Керівник пошукової
бригади**

_____/_____/

Члени пошукової бригади

_____/_____/

" ____ " _____ 20__ г.

**ПЕРЕЛІК НОРМАТИВНО-ПРАВОВИХ ДОКУМЕНТІВ
на основі яких здійснюється діяльність
за поданням послуг з ТЗІ**

1. Закон України "Про інформацію".
<https://zakon.rada.gov.ua/laws/main/2657-12>
2. Закон України "Про доступ до публічної інформації".
3. Закон України "Про захист інформаційно- телекомунікаційних системах". <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
4. За Закон України "Про основні засади забезпечення кібербезпеки України" <https://zakon.rada.gov.ua/laws/main/2163-19>
5. Закон України "Про електронні документи та електронний документообіг". <https://zakon.rada.gov.ua/laws/show/851-15>
6. Постанова Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 № 373. <https://zakon.rada.gov.ua/laws/main/373-2006-%D0%BF>
7. Постанова Кабінету Міністрів України "Про затвердження Порядку підключення до глобальних мереж передачі даних" від 12.04.2002 р. № 522.
8. Постанова Кабінету Міністрів України "Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних" від 04.02.1998 № 121. <https://zakon.rada.gov.ua/laws/main/121-98-%D0%BF>
9. Постанова Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.2010 № 518.
10. Постанова Кабінету Міністрів України "Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію" від 19 жовтня 2016 р. № 736.
11. ДСТУ 33960-96. Захист інформації. Технічний захист інформації. Основні положення.
http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?artid=38911&cat_id=38836
12. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?artid=38911&cat_id=38836

13. НД 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

<https://zakon.rada.gov.ua/rada/show/v0215519-13>

14. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=302408&cat_id=89734&ctime=1547122731920

15. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=89740&cat_id=89734&ctime=1547204009788

16. НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації.

17. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі. http://www.dut.edu.ua/uploads/I_1023_75718671.pdf

18. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

19. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

<http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342>

20. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (зі зміною № 1).

http://dstszi.kmu.gov.ua/dstszi/control/uk/publishvarticle?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407

21. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу "2".

<http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106343>

22. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

<http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106344>

23. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв. <http://www.dsszzi.gov.ua/dsszzi/doccatalog/document%3Fid=103253>

24. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.

http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46075

25. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074

26. НД ТЗІ Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичним джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації.

http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101924&cat_id=89734&ctime=1344501363205

27. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ ПЕМВН-95).

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101798&cat_id=89734&ctime=1344500065981

28. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95).

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=120206&cat_id=89769&ctime=1421836194327

29. ДСТУ ISO/IEC 27001: 2015 Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001: 2013, IDT).

30. ДСТУ ISO/IEC 27002: 2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27003: 2013, IDT).

31. ДСТУ ISO/IEC 27005: 2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005: 2018, IDT).

32. Указ Президента України "Про Положення про технічний захист інформації в Україні" від 27.09.1999 № 1229.