

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ  
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ  
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ  
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ  
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ**

**КВАЛІФІКАЦІЙНА РОБОТА**

на тему:

«Технологія захисту інформації від витоку матеріально-речовим каналом»

на здобуття освітнього ступеня магістра  
зі спеціальності 125 Кібербезпека та захист інформації»  
(код, найменування спеціальності)  
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

*Кваліфікаційна робота містить результати власних досліджень.  
Використання ідей, результатів і текстів інших авторів мають посилання на  
відповідне джерело*

\_\_\_\_\_ Антон ІНЮШЕВ

Виконав: здобувач вищої освіти групи СЗДМ 61  
Антон ІНЮШЕВ

Керівник: Юрій ПЕПА  
к.т.н., доцент (Ім'я, ПРІЗВИЩЕ)

Рецензент: \_\_\_\_\_  
(Ім'я, ПРІЗВИЩЕ)

Київ 2025

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ  
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ  
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ  
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

Кафедра Технічних систем кіберзахисту  
 Ступінь вищої освіти магістр  
 Спеціальність Кібербезпека та захист інформації  
 Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

**ЗАТВЕРДЖУЮ**

Завідувач кафедри ТСКБ

Олександр ТУРОВСЬКИЙ

«    »                      2024 р.

**ЗАВДАННЯ  
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Інюшеву Антону Володимировичу

*(прізвище, ім'я, по батькові здобувача)*

1. Тема кваліфікаційної роботи:

«Технологія захисту інформації від витоку матеріально-речовим каналом»

керівник кваліфікаційної роботи Юрій ПЕПА к.т.н., доцент

*(Ім'я, ПРИЗВИЩЕ, науковий ступінь, вчене звання)*

затверджені наказом Державного університету інформаційно-комунікаційних технологій  
 від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи

20.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи:

Інформаційна безпека матеріально-речового каналу

Технічні засоби охорони як інструмент протидії витоку інформації матеріально-речовим каналом

Захист інформації від витоку матеріально-речовим каналом

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Загрози інформаційній безпеці матеріально-речового каналу

2. Функціональність технічної системи охорони

3. Технологія захисту інформації від витоку матеріально-речовим каналом

5. Перелік графічного матеріалу: Презентаційний матеріал на 14 слайдах

6. Дата видачі завдання

20.10.2024

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи  | Строк виконання етапів роботи | Примітка |
|-------|--------------------------------------|-------------------------------|----------|
| 1     | Підбір науково-технічної літератури  |                               |          |
| 2     | Написання першого розділу роботи     |                               |          |
| 3     | Написання другого розділу роботи     |                               |          |
| 4     | Написання третього розділу роботи    |                               |          |
| 5     | Написання висновків по роботі        |                               |          |
| 6     | Підготовка презентаційних матеріалів |                               |          |
| 7     | Підготовка доповіді                  |                               |          |

Здобувач вищої освіти

\_\_\_\_\_

(підпис)

Антон ІНЮШЕВ

(Ім'я, ПРІЗВИЩЕ)

Керівник роботи

\_\_\_\_\_

(підпис)

Юрій ПЕПА

(Ім'я, ПРІЗВИЩЕ)

## РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи: 74 стор., 19 рис., 17 джерел.

*Об'єкт дослідження* – Процес захисту інформації.

*Предмет дослідження* – Захист інформації від витоку матеріально-речовим каналом.

*Мета роботи* – Розробка технології захисту інформації від витоку матеріально-речовим каналом.

*Методи дослідження* – системний аналіз, чисельні методи.

У роботі розглянуто технічну систему охорони як інструмент захисту інформації від витоку матеріально-речовим каналом. Проаналізовано загрози витоку інформації матеріально-речовим каналом

Грунтуючись на проведеному дослідженні розроблено рекомендації по підвищенню ефективності захисту інформації від витоку матеріально-речовим каналом.

Галузь використання – захист інформації на об'єкті інформаційної діяльності.

### **Апробація:**

**Б.В. Чабан, А.В. Інюшев** Методи підвищення ефективності захисту інформації від витоку матеріально-речовим каналом на основі комплексування даних. *Всеукраїнської науково-практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем.* м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.17 - 18.

[https://duikt.edu.ua/uploads/p\\_2661\\_93669247.pdf](https://duikt.edu.ua/uploads/p_2661_93669247.pdf)

МАТЕРІАЛЬНО-РЕЧОВИЙ КАНАЛ, ТЕХНІЧНА СИСТЕМА ОХОРОНИ, ЗАГРОЗИ ІНФОРМАЦІЇ, ПАСИВНИЙ СПОВІЩУВАЧ, АКТИВНИЙ СПОВІЩУВАЧ.

## ABSTRACT

The text part of the bachelor's (master's) qualification work: 74 pages, 19 figures, 17 sources.

*The object of research* is the process of information protection.

*The subject of the research* is information protection against leakage through the physical channel.

*The purpose of the work* is to development of protection technology information against leakage through the physical channel.

*Research methods* – system analysis, numerical methods.

The paper examines the technical protection system as a tool to protect information from leakage through the physical channel. Threats of information leakage through the physical channel have been analyzed

Based on the conducted research, recommendations were developed to increase the effectiveness of information protection against leakage through the physical channel.

The field of use is the protection of information at the object of information activity.

Approbation:

B.V. Chaban, A.V. Inyushev Methods for increasing the effectiveness of information protection from leakage through a material channel based on data integration. All-Ukrainian scientific and practical conference: Current problems of information and telecommunication systems security. Kyiv, November 3, 2024, Kyiv: RVC DUKT. – 024. P.17 - 18.

[https://duikt.edu.ua/uploads/p\\_2661\\_93669247.pdf](https://duikt.edu.ua/uploads/p_2661_93669247.pdf)

MATERIAL CHANNEL, TECHNICAL PROTECTION SYSTEM, INFORMATION THREATS, PASSIVE DETECTOR, ACTIVE DETECTOR.

## ЗМІСТ

|                                                                                             |           |
|---------------------------------------------------------------------------------------------|-----------|
| <b>ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....</b>                                                       | <b>7</b>  |
| <b>ВСТУП.....</b>                                                                           | <b>8</b>  |
| <b>1 ІНФОРМАЦІЙНА БЕЗПЕКА ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ.....</b>                         | <b>9</b>  |
| 1.1 Загрози витоку інформації технічними каналами з об'єктів інформаційної діяльності.....  | 9         |
| 1.2 Матеріально-речовий канал витоку інформації.....                                        | 14        |
| 1.3 Шляхи захисту інформації на об'єктах інформаційної діяльності.....                      | 16        |
| <b>2 ФУНКЦІОНАЛЬНІСТЬ ТЕХНІЧНОЇ СИСТЕМИ ОХОРОНИ.....</b>                                    | <b>29</b> |
| 2.1 Способи побудови технічних систем охорони.....                                          | 29        |
| 2.2 Склад технічної системи охорони.....                                                    | 33        |
| 2.3 Технічні засоби контролю стану периметрів об'єктів.....                                 | 38        |
| 2.4 Технічні засоби контролю стану внутрішніх рубежів об'єкту інформаційної діяльності..... | 48        |
| 2.5 Засоби прийому та обробки сигналів сповіщувачів.....                                    | 54        |
| <b>3 ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ.....</b>          | <b>61</b> |
| <b>ВИСНОВКИ.....</b>                                                                        | <b>71</b> |
| <b>ПЕРЕЛІК ПОСИЛАНЬ.....</b>                                                                | <b>72</b> |

## **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ**

ВПОС - виносний пристрій оптичної сигналізації

ІзОД – інформація з обмеженим доступом

ІЧ – інфрачервоне

КП – контрольна панель

МКС – магнітоконтактний сповіщувач

МР – матеріально-речовий

ОІД – об’єкт інформаційної діяльності

ПІЧ – пасивний інфрачервоний

ППКОП - прилад прийомо-контрольний охоронно пожежний

СП – сейсмоприймач

СЗВ – сейсмічні засоби виявлення

СЗОІ - система збору й обробки інформації

ТСО – технічна система охорони

## ВСТУП

*Актуальність дослідження.* Увага до питань інформаційної безпеки зростає, дослідження в цій сфері свідчать про намагання збалансувати зусилля щодо зниження ризиків з підвищенням ефективності діяльності. Важливо усвідомлювати ефективність стану захищеності ресурсів на об'єктах інформаційної діяльності підприємства, для протистояння різним видам загроз інформації.

Виходячи з цього, необхідність здійснення постійного аналізу загроз та моніторинг нових засобів безпеки інформації вкрай необхідна.

Одним із шляхів витоку інформації є матеріально-речовий канал, що може принести великих фінансових втрат якщо буде порушена безпека інформації у ньому.

У зв'язку з цим можна зробити висновок, що тема магістерської роботи, присвяченої підвищенню ефективності захисту інформації від витоку матеріально-речовим каналом є актуальною.

*Об'єкт дослідження* – Процес захисту інформації.

*Предмет дослідження* – Технічна система захисту інформації від витоку матеріально-речовим каналом.

*Мета роботи* – Підвищити ефективність захисту інформації від витоку матеріально-речовим каналом.

*Наукові завдання:*

зробити аналіз загроз витоку інформації матеріально-речовим каналом;  
проаналізувати функціональність технічних засобів охорони об'єктів;  
розробити ефективну систему захисту інформації від витоку матеріально-речовим каналом за рахунок застосування ТЗОО.

*Методи дослідження* – системний аналіз, чисельні методи.

*Практичне значення одержаних результатів* полягає у розробці технічної системи захисту інформації від витоку матеріально-речовим каналом з підвищеною ефективністю.



## Розділ 1.

# ІНФОРМАЦІЙНА БЕЗПЕКА ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

## 1.1 Загрози витоку інформації технічними каналами з об'єктів інформаційної діяльності

Об'єкт інформаційної діяльності, за визначенням [1], [2] це будівля або інженерна споруда де здійснюється обіг та зберігання ІзОД.

Для негласного отримання інформації на практиці використовуються різні технічні засоби. Інформація з об'єкта надходить злоумисникові по різним фізичним каналам.

- Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення і використовуваних технічних засобів, технічні канали витоку бувають: м

- матеріально-речовий.
- акустичний;
- радіоканал;
- електричний;
- оптичний;

Радіоканали утворюються за рахунок:

- магнітного поля;
- паразитної генерації;
- по ланцюгах живлення;
- по ланцюгам заземлення;
- електромагнітного випромінювання.

Взагалі склад будь якого технічного каналу витоку інформації в загальному випадку включає в себе (рис. 1.1): джерело сигналу або передавач, середу поширення сигналу і отримувач сигналу [4].



Рис. 1.1 Склад технічного каналу витоку інформації

В радіоканалах витоку інформації джерела сигналів можуть бути чотирьох видів:

- передавачі функціональних каналів зв'язку;
- джерела небезпечних сигналів;
- об'єкти, що відображають енергію радіочастоти;
- об'єкти, що випромінюють власні (теплові) радіохвилі.

Середовищем поширення радіоелектронного каналу витоку інформації є атмосфера, безповітряний простір. Носій у вигляді електромагнітного поля поширюється в атмосфері, в безповітряному просторі або по направляючим - хвильоводам. У приймачі проводиться виділення (селекція) носія з цікавою одержувачу інформацією по частоті, посилення виділеного слабкого сигналу і зняття з нього інформації - демодуляція.

При перехопленні сигналів функціональних каналів зв'язку передавачі цих каналів є одночасно джерелами радіоканалів витоку інформації. У загальному випадку напрям поширення електромагнітної хвилі від передавача до санкціонованого одержувача і зловмисникові відрізняються. У функціональних каналах зв'язку максимум випромінювання енергії електромагнітної хвилі орієнтують в напрямку розташування приймача санкціонованого одержувача. Тому потужність джерела сигналів радіоканалу витоку інформації, як правило, істотно менше потужності випромінювання в функціональному каналі зв'язку.

Причини виникнення електричних каналів витоку інформації:

- наведення побічних електричних випромінювань ОТЗ на з'єднувальні лінії ДТЗС і сторонні провідники;

- наведення побічних електричних випромінювань ОТЗ на ланцюзі електроживлення і заземлення ОТЗ;
- «просочування» інформаційних сигналів у колі електроживлення і заземлення ОТЗ.

Одним з видів технічних каналів витоку інформації, що виникають при роботі засобів і систем інформатизації (електронно-обчислювальна, телевізійна й інша техніка), є канали, що з'являються за рахунок побічних електромагнітних випромінювань і наведень [3]. До найбільш поширених шляхів витоку інформації внаслідок наведень відносяться канали, які утворюються в мережі електроживлення технічних засобів і систем.

Крім заземлюючих провідників, які слугують для безпосереднього з'єднання ОТЗ з контуром заземлення, гальванічний зв'язок з землею можуть мати різні провідники, що виходять за межі контрольованої зони. До них відносяться нульовий провід мережі електроживлення, екрани (металеві оболонки) з'єднувальних кабелів, металеві труби систем опалення та водопостачання, металева арматура залізобетонних конструкцій і т.д. Всі ці провідники разом з заземлювальним пристроєм утворюють розгалужену систему заземлення, на яку можуть наводитися інформаційні сигнали. Крім того, в ґрунті навколо заземлювального пристрою виникає електромагнітне поле, яке також є джерелом інформації.

Перехоплення інформаційних сигналів в лініях електроживлення і колах заземлення ОТЗ можливий при гальванічному підключенні до них засоби розвідки потенційного порушника інформаційної безпеки.

Одна з основних причин утворення шляхів витоку інформації лініями заземлення пов'язана з тим, що перераховані типи заземлення рідко вдається виконати відокремленими. Поєднання декількох функцій однієї системою провідників і провідних поверхонь призводить до того, що по ним відбуваються різні струми, в тому числі і небезпечні. У загальному випадку небезпечними потоками є зворотні струми для різних сигналів основних технічних засобів і систем, а також струми, обумовлені наведеннями небезпечних сигналів на лінію

заземлення. Причому найбільшу небезпеку представляють зворотні струми, так як вони можуть мати досить велику величину.

Акустичні канали витоку інформації утворюються за рахунок:

- поширення акустичних коливань у вільному повітряному просторі;
- впливу звукових коливань на елементи і конструкції будівель;
- впливу звукових коливань на технічні засоби.

Механічні коливання стін, перекриттів, трубопроводів, що виникають в одному місці від впливу на них джерел звуку, передаються по будівельним конструкціям на значні відстані, майже не затухаючи, і випромінюються в повітря як чутний звук. Небезпека такого акустичного каналу витоку інформації з елементів будівлі полягає в великій і неконтрольованій дальності поширення звукових хвиль, перетворених в пружні поздовжні хвилі в стінах і перекриттях, що дозволяє прослуховувати розмови на значних відстанях.

Ще один шлях витоку акустичної інформації утворюють системи повітряної вентиляції приміщень, різні витяжні системи та системи подачі чистого повітря. Можливість виникнення таких каналів визначаються конструктивними особливостями повітропроводів і акустичними характеристиками їх елементів: засувки, переходів, розподільників і ін.

Залежно від фізичної природи виникнення інформаційних сигналів, середовища поширення акустичних коливань і способів їх перехоплення, акустичні канали витоку інформації також можна розділити на повітряні, вібраційні, електроакустичні, оптико-електронні та параметричні [4].

У повітряних технічних каналах витоку інформації середовищем поширення акустичних сигналів є повітря, а для їх перехоплення використовуються мініатюрні високочутливі мікрофони і спеціальні спрямовані мікрофони.

Перехоплена інформація може також передаватися по радіоканалу, оптичного каналу (в інфрачервоному діапазоні довжин хвиль), по мережі змінного струму, з'єднувальним лініях ДТЗС. Причому для передачі інформації

по трубах і металоконструкціях можуть застосовуватися не тільки електромагнітні, а й механічні коливання.

У вібраційних каналах витоку інформації середовищем поширення акустичних сигналів є конструкції будівель, споруд (стіни, стелі, підлоги), труби водопостачання, опалення, каналізації та інші тверді тіла. Для перехоплення акустичних коливань в цьому випадку використовуються електричні мікрофони (стетоскопи).

Електроакустичні технічні канали витоку інформації виникають за рахунок електроакустичних перетворень акустичних сигналів в електричні. Перехоплення акустичних коливань здійснюється через ДТЗС, що володіють "мікрофонним ефектом" (перетворення акустичних мовних коливань повітряного середовища в електричні сигнали), а також шляхом "високочастотного нав'язування".

Оптико-електронний шлях витоку інформації утворюється при опроміненні лазерним променем вібруючих в акустичному полі тонких відображаючих поверхонь (скла, вікон, картин, дзеркал і т.д.). Відбите лазерне випромінювання (дифузне або дзеркальне) модулюється за амплітудою і фазою (згідно із законом вібрації поверхні) і приймається приймачем оптичного випромінювання, при демодуляції якого виділяється мовна інформація.

Візуально-оптичне спостереження є найбільш відомим, досить простим, широко поширеним і добре оснащеним найсучаснішими технічними засобами розвідки.

Ці особливості визначають небезпеку даного виду каналів витоку інформації. Оптичні методи є одними з найстаріших методів отримання інформації.

До них відносяться:

- візуальні методи спостереження;
- фотозйомка;
- відеозйомка.

Ці методи дозволяють отримувати інформацію як в звичайних умовах, так і при мінімальній освітленості, в інфрачервоному спектрі і за допомогою термографії, а також в повній темряві. В даний час для збору інформації по візуально-оптичним каналам широко застосовують волоконні світловоди і світлочутливі мікросхеми. Сучасні системи фотозйомки і відеозйомки дозволяють здійснювати дистанційне керування. Розроблено системи, здатні проводити зйомку практично в абсолютній темряві, що дозволяють фотографувати через найменші отвори.

## **1.2 Матеріально-речовий канал витоку інформації**

Матеріально-речовий канал витоку інформації знаходиться на особливому положенні серед решти. Це пов'язано зі специфічністю його виникнення.

У даному випадку застосовується отримання інформації з відходів виробничої та трудової діяльності. Залежно від профілю роботи підприємства це можуть бути зіпсовані накладні, фрагменти складаються документів, чернетки листів, браковані заготовки деталей, панелей, кожухів та інших пристроїв для розроблюваних підприємством нових моделей різної техніки. Особливе місце серед такого роду джерел займають залишки бойової техніки і озброєння на випробувальних полігонах.

За своїм фізичним станом відходи виробництва можуть являти собою тверді маси, рідини і газоподібні речовини; по фізичній природі вони діляться на хімічні, біологічні, радіаційні, а по середовищу поширення на що містяться в землі, у воді і в повітрі.

Особливість матеріально-речового каналу, в порівнянні з іншими каналами, обумовлена специфікою джерел і носіїв видобувається по ньому інформації. Джерелами і носіями інформації в даному випадку є суб'єкти (люди) і матеріальні об'єкти (макро- і мікрочастинки), які мають чіткі просторові межі локалізації (за винятком випромінювань радіоактивних речовин). Витік

інформації по матеріально-речовим каналах супроводжується фізичним переміщенням людей і матеріальних тіл з інформацією за межі об'єкта, що захищається.

Основними джерелами інформації матеріально-речового каналу витоку інформації є:

- чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв, що розробляються в ході науково-дослідних і дослідно-конструкторських робіт, які ведуться в організації;
- вийшли з ладу магнітні та інші носії інформації ПЕОМ, на яких під час експлуатації містилася інформація з обмеженим доступом;
- бракована продукція та її елементи;
- секретні бібліотеки;
- інші місця зберігання матеріальних носіїв ІзОД.

Перенесення інформації в матеріально-речовому каналі може здійснюватися [4]:

- співробітниками організації;
- повітряними атмосферними масами;
- рідкими середовищами.

Втрата носіїв цінної інформації можлива за відсутності в організації чіткої системи їх обліку. Наприклад, друкарка, зіпсувавши аркуш звіту, викидає його в кошик для сміття, з якої він переноситься прибиральницею в сміттєвий бак, що знаходиться на території організації. Потім при вантаженні або продовження транспортування сміття лист несеться вітром і потрапляє в руки випадкового перехожого. Звичайно, ймовірність забезпечення випадкового ознайомлення зловмисника з вмістом цього листа невелика. Однак якщо зловмисник активно займається добуванням інформації, область простору, в якій можливий контакт, значно звужується, що призводить до підвищення ймовірності витоку інформації по матеріально-речовим каналам.

Витік інформації через матеріально-речові канали витоку інформації можливий через:

- розкрадання носіїв інформації;
- внутрішні шляхи витоку (через обслуговуючий персонал);
- погано приховану видову інформацію про хід виробничого процесу на підприємстві.

Для добування інформації зловмисник, як правило, використовує кілька шляхів її витоку. Комплексне використання шляхів витоку інформації ґрунтується на наступних принципах:

- комплексируємі канали доповнюють один одного за своїми можливостями;
- ефективність комплексування підвищується при зменшенні залежності між джерелами інформації та демаскуючими ознаками в різних каналах.

Комплексування каналів витоку інформації забезпечує:

- збільшення ймовірності виявлення і розпізнавання об'єктів за рахунок розширення їх поточних ознакових структур;
- підвищення достовірності семантичної інформації і точності вимірювання ознак, особливо у разі добування інформації з недостатньо надійних джерел.

### **1.3 Шляхи захисту інформації на об'єктах інформаційної діяльності**

Як показано вище, при використанні на ОІД засобів технічної обробки та зберігання інформації (ІТС) має місце виникнення електричного, радіоканалу та матеріально-речового каналів витоку інформації на ОІД.

Існують наступні методи та засоби протидії такому явищу.

Екранування технічних засобів.

Функціонування будь-якого технічного засобу інформації пов'язано з протіканням по його струмоведучих елементів електричних струмів різних частот і утворенням різниці потенціалів між різними точками його електричної схеми, які породжують магнітні та електричні поля, так звані побічні електромагнітні випромінювання.



Зниженню рівня побічних електромагнітних випромінювань приділяється велика увага.

Ефективним методом зниження рівня ПЕМВ є екранування їх джерел.

Електростатичне і магнітостатичне екранування засновані на замиканні екраном відповідно електричного і магнітного полів.

Електростатичне екранування по суті зводиться до замикання електростатичного поля на поверхню металевого екрана і відведення електричних зарядів на землю (на корпус приладу). Заземлення електростатичного екрана є необхідним елементом при реалізації електростатичного екранування. Застосування металевих екранів дозволяє повністю усунути вплив електростатичного поля.

Основним завданням екранування електричних полів є зниження ємності зв'язку між екрануючими елементами конструкції. Отже, ефективність екранування визначається в основному ставленням ємностей зв'язку між джерелом і рецептором наведення до і після установки заземленого екрану. Тому будь-які дії, що призводять до зниження ємності зв'язку, збільшують ефективність екранування.

Магнітостатичне екранування використовується при необхідності придушити наведення на низьких частотах від 0 до 3 ... 10 кГц.

Основні вимоги, що пред'являються до магнітостатичних екранів, можна звести до наступних:

- магнітна проникність матеріалу екрану повинна бути якомога вищою.
- збільшення товщини стінок екрану призводить до підвищення ефективності екранування, однак при цьому слід брати до уваги можливі конструктивні обмеження за масою і габаритами екрану;
- стики, розрізи і шви в екрані повинні розміщуватися паралельно лініям магнітної індукції магнітного поля. Їх кількість має бути мінімальною;
- заземлення екрана не впливає на ефективність магнітостатичного екранування.

Ефективність магнітного екранування залежить від частоти і електричних властивостей матеріалу екрану. Чим нижче частота, тим слабкіше діє екран, тим більшої товщини доводиться його робити для досягнення одного і того ж екрануючого ефекту.

При екранування магнітного поля заземлення екрана не змінює величини порушуваних в екрані струмів і, отже, на ефективність магнітного екранування не впливає.

На високих частотах застосовується виключно електромагнітне екранування. Дія електромагнітного екрану засноване на тому, що високочастотне електромагнітне поле послаблюється їм же створеним полем зворотного напрямку.

Також екрануванню підлягають монтажні дроти і сполучні лінії. Щоб зменшити рівень ПЕМВ, необхідно особливо ретельно виконувати з'єднання оболонки дрота (екрану) з корпусом апаратури. Підключення оболонки має здійснюватися шляхом безпосереднього контакту (найкраще шляхом пайки або зварювання) з корпусом.

У звичайних (неекранованих) приміщеннях основний екрануючий ефект забезпечують залізобетонні стіни будинків. Екрануючі властивості дверей і вікон гірші. Для підвищення екрануючих властивостей стін застосовуються додаткові засоби, в тому числі:

- струмопровідні лакофарбові покриття або струмопровідні шпалери;
- штори з металізованої тканини;
- металізоване скло, що встановлюються в металеві або металізовані рами.

Фільтрація інформаційних сигналів як пасивний метод захисту від витoku інформації електричним каналом.

Одним з методів локалізації небезпечних сигналів, що циркулюють в технічних засобах і системах обробки інформації, є фільтрація. У джерелах електромагнітних полів і наведень фільтрація здійснюється з метою запобігання поширенню небажаних електромагнітних коливань за межі пристрою - джерела

небезпечного сигналу. Фільтрація в пристроях - рецепторах електромагнітних полів і наведень повинна виключити їх вплив на рецептор.

Для фільтрації сигналів в ланцюгах живлення ТСПІ використовуються розділові трансформатори і шумопридушуючі електричні фільтри.

Розділові трансформатори повинні забезпечувати розв'язку первинної та вторинної ланцюгів за сигналами наводки [4]. Це означає, що у вторинний ланцюг трансформатора не повинні проникати наведення, що з'являються в ланцюзі первинної обмотки. Проникнення наведень у вторинну обмотку пояснюється наявністю небажаних резистивних і ємнісних ланцюгів зв'язку між обмотками.

Для зменшення зв'язку обмоток за сигналами наведень часто застосовується внутрішній екран, який виконан у вигляді заземленої прокладки або фольги, що укладається між первинною і вторинною обмотками. За допомогою цього екрана наводка, діюча в первинній обмотці, замикається на землю. Однак електростатичне поле навколо екрану також може служити причиною проникнення наведень у вторинний ланцюг.

Розділові трансформатори використовуються з метою вирішення ряду завдань, в тому числі для:

- поділу по ланцюгах живлення джерел і рецепторів наведення, якщо вони підключаються до одних і тих же шин змінного струму;
- усунення асиметричних наведень;
- ослаблення симетричних наведень в ланцюзі вторинної обмотки, обумовлених наявністю асиметричних наведень в ланцюзі первинної обмотки.

В даний час існує велика кількість різних типів фільтрів, що забезпечують ослаблення небажаних сигналів в різних ділянках частотного діапазону. Це фільтри нижніх і верхніх частот, смугові та загороджуючі фільтри. Основне призначення фільтрів - пропускати без значного ослаблення сигнали з частотами, що лежать в робочій смузі частот, і пригнічувати (послаблювати) сигнали з частотами, що лежать за межами цієї смуги. Для виключення просочування

інформаційних сигналів у колі електроживлення використовуються фільтри нижніх частот.

Основні вимоги, що пред'являються до захисних фільтрів, полягають в наступному:

- величини робочої напруги і струму фільтра повинні відповідати напрузі і струму фільтрованого ланцюга;
- величина послаблення небажаних сигналів в діапазоні робочих частот повинна бути не менше необхідної;
- послаблення корисного сигналу в смузі прозорості фільтра має бути незначним;
- габарити і маса фільтрів повинні бути мінімальними;
- фільтри повинні забезпечувати функціонування за певних умов експлуатації (температура, вологість, тиск) і механічних навантажень (удари, вібрація і т.д.);
- конструкції фільтрів повинні відповідати вимогам техніки безпеки.

Просторове і лінійне зашумлення як методи активного захисту інформації від витоків електричним та радіоканалом.

Реалізація пасивних методів захисту, заснованих на застосуванні екранування і фільтрації, призводить до ослаблення рівнів побічних електромагнітних випромінювань і наведень (небезпечних сигналів) ОТЗ і тим самим до зменшення відносини небезпечний сигнал / шум (с / ш). Однак в ряді випадків, незважаючи на застосування пасивних методів захисту, на кордоні контрольованої зони відношення с / ш перевищує допустиме значення. У цьому випадку застосовуються активні заходи захисту, засновані на створенні перешкод засобом розвідки, що також призводить до зменшення відносини с / ш.

Для виключення перехоплення побічних електромагнітних випромінювань по електромагнітному каналу використовується просторове зашумлення, а для виключення знімання наведень інформаційних сигналів з сторонніх провідників і сполучних ліній допоміжних технічних засобів - лінійне зашумлення.

До системи просторового зашумлення, яка застосовується для створення маскувальних електромагнітних перешкод, висуваються такі вимоги:

- система повинна створювати електромагнітні перешкоди в діапазоні частот можливих побічних електромагнітних випромінювань ОТЗ;
- створювані перешкоди не повинні мати регулярну структури;
- рівень створюваних перешкод (як по електричній, так і по магнітної складової поля) повинен забезпечити ставлення  $s / \text{ш}$  на кордоні контрольованої зони менше допустимого значення у всьому діапазоні частот можливих побічних електромагнітних випромінювань ОТЗ;
- система повинна створювати перешкоди як з горизонтальною, так і з вертикальною поляризацією;
- на кордоні контрольованої зони рівень перешкод, створюваних системою просторового зашумлення, не повинен перевищувати встановлених норм по електромагнітній сумісності(ЕМС).

Мета просторового зашумлення вважається досягнутою, якщо відношення небезпечний сигнал / шум на кордоні контрольованої зони не перевищує деякого допустимого значення, що розраховується за спеціальними методиками для кожної частоти інформаційного (небезпечного) побічного електромагнітного випромінювання ОТЗ.

У системах просторового зашумлення в основному використовуються слабонаправлені рамкові жорсткі і гнучкі антени. Рамкові гнучкі антени виконуються зі звичайного дроту і розгортаються в двох-трьох площинах, що забезпечує формування завадового сигналу як з вертикальною, так і з горизонтальною поляризацією в усіх площинах.

Системи лінійного зашумлення застосовуються для маскування наведених небезпечних сигналів в сторонніх провідниках і з'єднувальних лініях ДТЗС, що виходять за межі контрольованої зони.

У найпростішому випадку система лінійного зашумлення представляє собою генератор шумового сигналу, який формує шумову маскуючу напруга із заданими спектральними, тимчасовими і енергетичними характеристиками, який

гальванічно підключається в зашумлюючу лінію (сторонній провідник). На практиці найбільш часто подібні системи використовуються для зашумлення ліній електроживлення.

Методи протидії від витоку інформації по акустичному каналу діляться на активні та пасивні.

Захист мовної інформації є важливим завданням в загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єкта чи установи.

Для її перехоплення «противник» може використовувати широкий арсенал портативних засобів акустичної мовної розвідки, які дозволяють перехоплювати мовну інформацію по прямому акустичному, віброакустичному, електроакустичному і оптико-електронного (акустооптичні) каналам до основних з яких відносяться:

- портативна апаратура звукозапису (малогабаритні диктофони, магнітофони та пристрої запису на основі цифрової схемотехніки);
- спрямовані мікрофони;
- електронні стетоскопи;
- електронні пристрої перехоплення мовної інформації (закладні пристрої) з датчиками мікрофонного і контактного типів з передачею перехопленої інформації по радіо, оптичному (в інфрачервоному діапазоні довжин хвиль) і ультразвуковому каналам, мережі електроживлення, телефонних лініях зв'язку, з'єднувальних лініях допоміжних технічних засобів або спеціально прокладених лініях;
- оптико-електронні (лазерні) акустичні системи й т.п.

Використання тих чи інших методів і засобів визначається характеристиками об'єкта захисту і апаратури розвідки, умовами її ведення, а також вимог, що пред'являються до ефективності захисту акустичної (мовної) інформації, як показник оцінки якої використовується словесна розбірливість мови на виході каналу витоку інформації.

Пасивні методи захисту інформації.

Визначено, що для зниження розбірливості мови необхідно прагнути до зменшення відношення «рівень мовного сигналу / рівень шуму» (сигнал / шум) в місцях можливого розміщення датчиків апаратури акустичної розвідки.

Зменшення відношення сигнал / шум можливо наступними способами:

- пасивні методи захисту (зменшення) рівня мовного сигналу);
- активні методи захисту (збільшення рівня шуму).

Ослаблення акустичних (мовних) сигналів здійснюється шляхом звукоізоляції приміщень, яка спрямована на локалізацію джерел акустичних сигналів всередині них.

Звукоізоляція оцінюється величиною ослаблення акустичного сигналу і забезпечується за допомогою архітектурних та інженерних рішень, а також застосуванням спеціальних будівельних та оздоблювальних матеріалів. У разі якщо звукоізоляція приміщення не забезпечує необхідної ефективності захисту інформації, то для її підвищення використовують спеціальні звукопоглинаючі матеріали. Підвищення звукоізоляції стін і перегородок приміщення також досягається установкою на відстані в 6 ... 10 см від них одношарових і багатошарових (частіше подвійних) огорожень.

Одним з найбільш слабких звукоізолюючих елементів огорожувальних конструкцій виділених приміщень є двері і вікна.

Пасивні методи захисту інформації, як правило, реалізуються при будівництві або реконструкції будівель на етапі розробки проектних рішень, що дозволяє заздалегідь врахувати типи будівельних конструкцій, способи прокладки комунікацій, оптимальні місця розміщення виділених приміщень. У разі технічної неможливості використання пасивних засобів захисту приміщень або якщо вони не забезпечують необхідних норм по звукоізоляції, використовуються активні заходи захисту.

Активні методи захисту акустичної інформації.

Якщо необхідно проводити захист приміщення по акустичному каналу, слід впливати на середу поширення. Для цієї мети використовуються акустичні генератори шуму. Крім того, генератори шуму широко використовуються для

оцінки акустичних властивостей приміщень. Під акустичним шумом розуміють шум, який характеризується нормальним розподілом амплітудного спектра і постійністю спектральної щільності потужності на всіх частотах. Для зашумлення приміщень широко застосовуються перешкоди, що представляють собою суміш випадкових і нерівномірних періодичних процесів.

За принципом дії всі технічні засоби просторового і лінійного зашумлення можна розділити на три великі групи [4]:

Засоби створення акустичних маскуючих перешкод:

- генератори шуму в акустичному діапазоні;
- пристрої віброакустичного захисту;
- технічні засоби ультразвукового захисту приміщень.

Засоби створення електромагнітних маскуючих перешкод:

- технічні засоби просторового зашумлення;
- технічні засоби лінійного зашумлення, які діляться на засоби

створення маскуючих перешкод в комунікаційних мережах і засоби створення маскуючих перешкод в мережах електроживлення.

Багатофункціональні засоби захисту.

Найбільш ефективним засобом захисту приміщень, призначених для проведення конфіденційних заходів, від знімання інформації через шибки, стіни, системи вентиляції, труби опалення, двері і т.п. є пристрої віброакустичного захисту [3]. Дана апаратура дозволяє запобігти прослуховуванню за допомогою дротових мікрофонів, звукозаписуючої апаратури, радіомікрофонів і електронних стетоскопів, систем лазерного знімання акустичної інформації з вікон і т.п. Протидія прослуховуванню забезпечується внесенням віброакустичних шумових коливань в елементи сигналу.

Відмінною особливістю технічних засобів ультразвукового захисту приміщень є вплив на мікрофонний пристрій і його підсилювач достатньо сильним ультразвуковим сигналом, що викликає блокування підсилювача або виникнення значних нелінійних спотворень, що призводять, в кінцевому випадку, до порушення працездатності мікрофонного пристрою. Оскільки вплив



здійснюється по каналу сприйняття акустичного сигналу, то абсолютно не важливі його подальші трансформації і способи передачі. Акустичний сигнал пригнічується саме на етапі сприйняття чутливим елементом. Все це робить комплекс достатньо універсальним в порівнянні з іншими засобами активного захисту.

Захист від вбудованих і вузькоспрямованих мікрофонів. Мікрофони, як відомо, перетворюють енергію звукового сигналу в електричні сигнали. У сукупності зі спеціальними підсилювачами і фільтруючими елементами вони використовуються в якості пристроїв аудіоконтролю приміщень. Для цього створюється прихована провідна лінія зв'язку (або використовуються деякі з наявних в приміщенні провідних ланцюгів), виявити яку можна лише фізичним пошуком або за допомогою контрольних вимірів сигналів у всіх проводах, наявних в приміщенні. Звичайно, що методи радіоконтролю, ефективні для пошуку радіозакладок, в даному випадку не мають сенсу.

Для захисту від вузько спрямованих мікрофонів рекомендуються такі заходи:

- при проведенні нарад слід обов'язково закривати вікна і двері (найкраще, щоб кімната для нарад представляла собою ізольоване приміщення);
- для проведення переговорів потрібно вибирати приміщення, стіни яких не є зовнішніми стінами будівлі;
- необхідно забезпечити контроль приміщень, що знаходяться на одному поверсі з кімнатою для нарад, а також приміщень, що знаходяться на суміжних поверхах.

Класифікація пристроїв пошуку технічних засобів розвідки може бути наступною:

Пристрої пошуку активного типу:

- нелінійні локатори (досліджують відгук на вплив електромагнітним полем).

Пристрої пошуку пасивного типу:

- пристрої та системи пошуку по електромагнітному випромінюванню;
- пристрої пошуку по зміні параметрів телефонної лінії (напруги, індуктивності, ємності, добротності);
- пристрої пошуку по зміні магнітного поля (детектори апаратури, що записує).

Спеціальні приймачі для пошуку працюючих передавачів в широкому діапазоні частот називають скануючими пристроями [3]. З активних засобів пошуку апаратури прослуховування в основному використовують нелінійні локатори. Принцип їх дії заснований на тому, що при опроміненні радіоелектронних пристроїв, що містять нелінійні елементи, такі, як діоди, транзистори і т.п., відбувається відображення сигналу на вищих гармоніках. Відбиті сигнали реєструються локатором незалежно від режиму роботи радіоелектронного пристрою, тобто незалежно від того, включено воно або вимкнено.

Вирішення задач пов'язаних із запобіганням витоків інформації матеріально-речовим каналом з об'єктів інформаційної діяльності полягає у використанні фізичної та технічної складових.

Одним з елементів технічної складової є технічні засоби охорони об'єктів які і являються предметом досліджень дипломної роботи.

Технічні засоби охорони поєднуються у технічну систему охорони яка призначена для [17]:

- постановки і зняття з охорони приміщень;
- формування та видачі сигналів тривоги при несанкціонованому появі або спробі проникнення людини в закриті і здані під охорону приміщення; перегляду стану охоронюваних приміщень на планах в графічній формі на автоматизованих робочих місцях (АРМ) інтегрованої системи безпеки (ІСБ) і відображення на них сигналів тривоги або несправності в графічному, текстовому та голосовому вигляді з прив'язкою до плану об'єкта;

- ведення протоколу подій системи ТСО в пам'яті комп'ютера з можливістю перегляду на моніторі і його роздруківки; ведення електронного журналу, фіксує дії операторів в стандартних і позаштатних ситуаціях.

У загальному вигляді технічна система охорони включає в себе наступні елементи (рис. 1.2) [4]:

- засіб виявлення;
- прилад приймально-контрольний охоронно пожежний (ППКОП);
- шлейф сигналізації;
- виконавчі пристрої - прилади, які забезпечують виконання заданого алгоритму дій системи у відповідь на ту чи іншу тривожну подію.



Рис. 1.2 Склад технічної системи охорони

Висновок по розділу. Проаналізовано існуючі шляхи витоку інформації. Загрозою витоку інформації матеріально-речовим каналом є крадіжка матеріальних носіїв. Для протидії витоку інформації матеріально-речовим каналом використовуються технічні системи охорони.

## Розділ 2.

## ФУНКЦІОНАЛЬНІСТЬ ТЕХНІЧНОЇ СИСТЕМИ ОХОРОНИ

### 2.1 Способи побудови технічних систем охорони

Структура типових варіантів побудови комплексів ТЗОС визначається розподілом логічної обробки інформації від ЗВ між станційною апаратурою і периферійними блоками (ПБ), а також способом зв'язку між ними і ЗВ [4]. На вибір варіанту структури побудови комплексу головним чином роблять вплив наступні чинники:

- якісний і кількісний склад обслуговуваних ЗВ і ПБ (концентратори, виносні пульти сигналізації і ін);
- ступінь централізації управління СЗОІ;
- структурні особливості об'єктів, що охороняються;
- чинники вартості і надійності.

Відомі наступні основні способи з'єднання станційної апаратури з периферійними блоками і ЗВ (варіанти побудови структурних схем ТЗО):

- радіальний (променевий) безконцентраторний;
- радіальний (променевий) з концентраторами;
- шлейфовий (магістральний) без концентраторів і з концентраторами;
- змішана (радіально-шлейфова).

Радіальний (променевий) безконцентраторний (рис. 2.1).

Як правило, комплекси ТЗОС з радіальною безконцентраторною структурою мають наступні основні особливості;

- простота виконання і технічного обслуговування апаратної частини (підключення, налаштування, ремонту і ін.);
- підключення кожного ЗВ здійснюється по окремих ланцюгах електроживлення, дистанційної перевірки і контролю стану;
- несправності, що виникають в лініях зв'язку ЗВ і вхідних ланцюгах станційної апаратури, впливають на працездатність тільки окремого каналу

сигналізації, що при відповідній організації охорони не впливає на функціонування всього комплексу ТЗОС;



Рис. 2.1 Радіальне (променеве) безконцентраторне з'єднання станційної апаратури із ЗВ

Радіальний (променевий) з концентраторами.

Призначення концентраторів в ТСО різного типу може відрізнятися по різних ознаках.

ПБ – периферійний блок

Окрім функцій збільшення ємності апаратури, тобто кількість одиничних апаратно-програмних ППКОП, кожне з яких призначене для контролю над станом одного ЗВ і ущільнення інформації що передається, концентратори можуть служити для об'єднання ЗВ по ділянках блокування, автоматичної перевірки їх працездатності і забезпечення контролю лінії зв'язку.

У окремих системах окрім названих функцій в концентратори закладаються функції попередньої обробки сигналів від ЗВ. Через них же здійснюється і електроживлення ЗВ.

Основна перевага комплексів з такою структурою – відносно низька вартість кабельних комунікацій і відносно короткий час їх монтажу.

Шлейфовий (магістральний) без концентраторів (рис. 2.2).

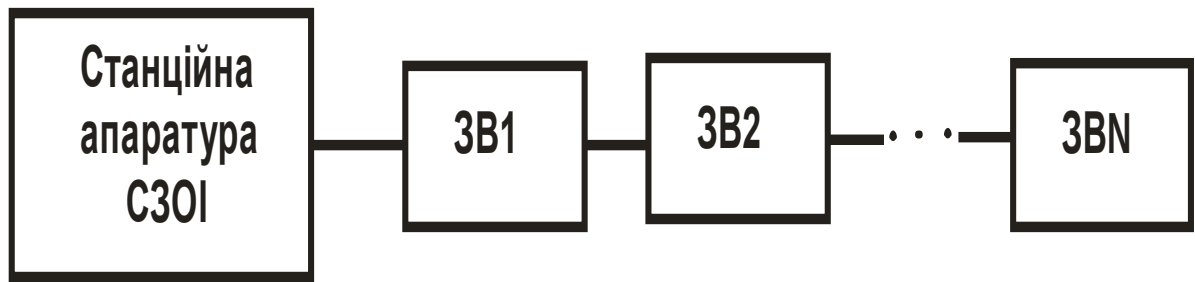


Рис. 2.2 Шлейфове (магістральне) без концентраторів  
з'єднання станційної апаратури із ЗВ

Працездатність комплексів ТЗОС з шлейфовою структурою у великій мірі визначається справним станом ліній зв'язку (у таких системах структура кабельних комунікацій менш розвинена, чим в радіальних ТЗОС), оскільки виникнення короткого замикання в лінії повністю порушує роботу комплексу, а у разі обриву в робочому стані залишається тільки та частина комплексу, з якою підтримується зв'язок [5]. Враховуючи дану обставину, останнім часом використовується резервування сполучних ліній і вузлів. При цьому подача електроживлення і зв'язок з пристроями комплексу здійснюється по двох незалежних шлейфах.

Тому при виході з ладу одного з них працездатність комплексу підтримується за рахунок іншого. Проте у цьому випадку вартість кабельних ліній і електромонтажних робіт збільшується практично в два рази. Також на працездатність комплексу ТЗОС з шлейфовою структурою великий вплив робить організація електроживлення ЗВ, оскільки живлення повинне подаватися по обмеженій кількості проводів і повинен враховуватися сумарний струм споживання всіх ЗВ і концентраторів (при їх наявності).

Змішана (радіально-шлейфова) або деревовидна структура.

Дана структура СЗОІ є комбінацією технічних засобів, сполучених по радіальній і шлейфовій схемам.

Необхідно відзначити, що вказані способи зв'язку периферійних блоків і ЗВ із станційною частиною СЗОІ можуть бути використані і для організації зв'язку ЗВ з ПБ. Зв'язок ПБ із ЗВ також може бути організований за допомогою

локальної мережі, що має шлейфову або деревовидну структуру. Для включення ЗВ на загальну магістраль локальної мережі необхідна розробка спеціальних блоків сполучення, що встановлюються поряд з кожним ЗВ і служать буфером між мережею і стандартизованими вихідними/вхідними ланцюгами ЗВ у вигляді контактів реле. Проте, часто вартість такого пристрою може бути сумірна з вартістю деяких ЗВ і перевищуватиме вигоду у вартості, що отримується за рахунок скорочення довжини кабелів зв'язку.

При виборі структури побудови комплексу ТЗОС враховуються:

- категорія об'єкта, що оснащується комплексом;
- витрати на устаткування об'єкта;
- рівень підготовленості персоналу, якому належить працювати зі встановлюваним комплексом;
- час пошуку і усунення несправностей і надійність лінії зв'язку для комплексів відносно невеликої ємності (до 100... 150 каналів), як правило, використовується радіальна схема з'єднання периферійних пристроїв і Із із станційною апаратурою, а для комплексів більшої ємності – шлейфова з концентраторами інформації сигналізації. При цьому обробка інформації повинна здійснюватися переважно в концентраторах, об'єднаних із станційною частиною по шинній структурі (локальній обчислювальній мережі).

Як правило, найбільш переважною є змішана структура побудови комплексів ТЗОС:

- для найбільш важливих ділянок блокування - радіальна структура;
- для менш важливих приміщень – шлейфова/магістральна структура.

У основі системи захисту об'єкту лежить принцип створення послідовних рубежів, в яких погрози мають бути своєчасно виявлені, а їх розповсюдженню повинні перешкоджати надійні перешкоди [6]. Такі рубежі (або зони безпеки) повинні розташовуватися послідовно - від огорожі навколо території об'єкту до головного, особливо важливого приміщення і інші.

Чим складніше і надійніше захист кожної зони безпеки, тим більше часу буде потрібно зловмисникові на її подолання і тим більше вірогідність того, що розташовані в зонах засоби виявлення загроз подадуть сигнал тривоги.

## 2.2 Склад технічної системи охорони

У загальному вигляді технічна система охорони включає в себе наступні засоби:

- засіб виявлення (ЗВ) (сповіщувач) - це пристрій, призначений для автоматичного формування сигналів із заданими параметрами (сигналу тривоги) внаслідок вторгнення або подолання зловмисником зони виявлення даного пристрою.
- прилад приймально-контрольний охоронно пожежний (ППКОП) - пристрій, який отримує сигнал тривоги від сповіщувачів та здійснює управління за заданим алгоритмом виконавчими пристроями (у простому випадку контроль за роботою охоронно-пожежної сигналізації складається з включення і виключення сповіщувачів, фіксації сигналів тривоги, в складних, розгалужених системах сигналізації контроль і управління здійснюються за допомогою комп'ютерів);
- шлейф сигналізації — електричний ланцюг, який поєднує сповіщувач з приладом приймально-контрольним охоронно-пожежним;
- виконавчі пристрої - агрегати, які забезпечують виконання заданого алгоритму дій системи у відповідь на ту чи іншу тривожну подію (подача сигналу оповіщення, включення механізмів пожежогасіння, автодозвон за заданими номерами телефонів і т.п.).

Основною складовою ТСО є сповіщувачі. Надалі представлена класифікація сповіщувачів.

Очевидно, при своєму русі людина-порушник залишає безліч різноманітних слідів свого руху і/або перебування, які можуть бути зафіксовані. Насправді, людина володіє цілком певними (кажучи в термінах математики,



розташованими в цілком певних областях існування) параметрами, як то: геометричними розмірами, масою, температурою тіла, запахом, електричними, біомеханічними і біодинамічними характеристиками, швидкостями руху, частотою кроку і ін..

При своєму русі він порушує звукові і ультразвукові коливання в атмосфері і навколишніх предметах, а також сейсмічні коливання в ґрунті і будівельних конструкцій. В процесі виконання тих або інших дій чоловік надає безпосередню силову дію на предмети, що цікавлять його, а також динамічну дію на поля електромагнітної і акустичної енергії, викликаючи порушення їх структури в просторі.

Рух людини супроводжується генерацією наднизькочастотних електричних полів, що виникають як наслідок перенесення індукованого в результаті тертя взуття об поверхню підлоги і взаємного тертя елементів тіла і одягу електростатичного заряду.

Крім того відомо, що в процесі фізичної діяльності чоловік випромінює електромагнітні сигнали в дуже широкому спектрі частот, а органи дихання і кровообігу генерують акустичні коливання. Потові залози людини виділяють в навколишню атмосферу продукти, у складі яких налічуються десятки хімічних речовин, деякі з яких є характерними тільки для людини.

В процесі проникнення в приміщення порушник відкриває двері, вікна, квартирки; іноді вимушений вирізувати і/або вибивати стекла, або проробляти отвори і проломи в стелях, підлозі або стінах. Усередині приміщення він пересуває предмети, обстановку, намагається розкрити металеві шафи або сейфи, фотографувати документи або вироби. Вказані чинники володіють самостійними інформативними характеристиками, що виявляють присутність (або сліди перебування) людини в приміщенні, що охороняється, одночасно збільшуючи об'єм інформації про нього.

Так, зброя, що є у порушника, або інструмент володіють певними фізичними параметрами і їх наявність може привести до зміни напруженості магнітного поля, частоти опромінюючого сигналу НВЧ. Застосування

механічного інструменту для відкриття дверей і металевих шаф, створення проломів і отворів в стінах і підлогах приміщень супроводиться збудженням характерних коливань (вібрацій) в твердих тілах і акустичних хвиль в повітряному середовищі приміщення.

При використанні газового пальника має місце теплове випромінювання полум'я, змінюється температура об'єкту на який діє порушник, з'являється специфічний запах горючої суміші, який, як і у разі застосування вибухових речовин, приводить до зміни хімічного складу повітря.

Таким чином, поява порушника в приміщенні, що охороняється, в загальному випадку може бути виявлене по великому числу фізикохімічних явищ. Це виявлення здійснюється за допомогою технічних засобів, в основу побудови яких покладені самі різні принципи реєстрації змін стану середовища.

Взагалі засоби виявлення класифікують за наступними ознаками:

1. За способом приведення в дію (постановка на охорону, зняття з охорони з центрального пульта) ЗВ підрозділяють на автоматичні і автоматизовані
2. За призначенням автоматичні ЗВ підрозділяють:
  - для закритих приміщень;
  - для відкритих майданчиків і периметрів об'єктів.
3. По виду зони, контрольованої ЗВ, виділяються:
  - лінійні;
  - поверхневі;
  - об'ємні (просторові).
4. За фізичним принципом дії розглядаються ЗВ наступних типів:
  - механічні (на практиці виділяють електроконтактні, магнітоконтактні, ударноконтактні);
    - ємнісні;
    - акустичні;
    - сейсмічні;
    - оптико-електронні;
    - радіохвильові;

- радіопроменеві (мікрохвильові);
- комбіновані.

5. По дальності дії ультразвукові, оптико-електронні і радіохвильові ЗВ для закритих приміщень розглядають:

- малої дальності дії – до 12 м;
- середньої дальності дії – понад 12 до 30 м;
- великої дальності дії – більше 30 м (окрім ультразвукових ЗВ).

6. По дальності дії оптико-електронні і радіохвильові ЗВ для відкритих майданчиків і периметрів об'єктів підрозділяють:

- малу дальність дії – до 50 м;
- середню дальність дії – понад 50 до 200 м;
- велику дальність дії – понад 200 м.

7. По конструктивному виконанню ультразвукові, оптико-електронні і радіохвильові ЗВ прийнято підрозділяти на:

- однопозиційні – один або більше передавачів (випромінювачів) і приймачів суміщені в одному блоці;
- двохпозиційні – передавач (випромінювач) і приймач виконані у вигляді окремих блоків;
- багатопозиційні – більше двох блоків (один передавач, два або більше приймачів; один приймач, два або більше передавачів; два або більше приймачів).

8. По принципу дії – активні (випромінюють радіо або інфрачервоне випромінювання), пасивні (працюють тільки на прийом випромінювань).

Кожен з названих класів ЗВ представлений на ринку безліччю різних датчиків, розрахованих для застосування в конкретних умовах.

Апріорі ясно, що вибір на ринку конкретного ЗВ виникає з відповідності його тактико-технічних характеристик (ТТХ) умовам застосування. Це означає, що ЗВ з даними (ТТХ) застосовують лише за певних умов, тобто ЗВ повинен бути встановлений в такому середовищі, характеристики якого (рельєф місцевості, електромагнітні поля, вібраційний фон, наявність або відсутність рослинності, параметри вологості, температури і так далі) в максимально

можливій мірі задовольняють можливостям вибраного ЗВ, визначуваним його ТТХ.

ТТХ повинні задовольняти умовам експлуатації, тобто безлічі таких чинників, як:

- кліматичні (вітер, пил, пісок, осадки, туман, тиск, сонячна радіація, температура, грозові та сезонні явища і ін.);
- біологічні (рослини, тварини, комахи, птахи);
- геологічні (рельєф місцевості, тип і хімічний склад ґрунту, водний простір, сейсмообстановка);
- механічні (вібрації, удари, прискорення);
- електромагнітні поля і випромінювання;
- акустичні коливання;
- рівень радіоактивності;
- режими роботи апаратури (інтенсивність, тимчасові параметри);
- умови електроживлення;
- рівень кваліфікації обслуговуючого персоналу і ін..;
- вартісні (розробки, виготовлення, монтажу і наладки, експлуатації) і багато що інше.

Виходячи з тих або інших чинників, обумовлюючих застосування ЗВ розглядають (закладають при розробці) наступні основні ТТХ:

- характеристики зони виявлення;
- вірогідність виявлення з вказана моделлю порушника;
- напрацювання на помилкове спрацьовування;
- чутливість ЗВ;
- параметри вхідних і вихідних сигналів;
- верхню і нижню межі швидкості переміщення порушника (об'єкту виявлення);
- час готовності ЗВ після включення напруги живлення;
- час відновлення чергового режиму після закінчення сигналу спрацьовування;

– показники надійності і ряд інших.

### **2.3 Технічні засоби контролю стану внутрішніх рубежів об'єкту інформаційної діяльності**

#### **Пасивні інфрачервоні засоби виявлення**

Пасивні інфрачервоні сповіщувачі руху чи сповіщувачі, відомі також за назвою оптико-електронні - найчастіше використовуються для виявлення руху в контрольованій зоні [6]. Це обумовлено досить високою ефективністю виявлення руху та низькою вартістю цих пристроїв. Ефективність виявлення проникнення в зону, що охороняється, визначається насамперед тим, що пасивні інфрачервоні сповіщувачі дозволяють контролювати весь об'єм приміщення.

Контроль об'єму всього приміщення – це не єдина задача, яку розв'язують ПІЧ-сповіщувачі. Використовуючи змінні лінзи (оптичні системи), можна ефективно контролювати вузьку смугу (наприклад, коридор) чи створити горизонтальну фіранку (наприклад, для контролю приміщень, у яких знаходяться домашні тварини) чи формувати вертикальну зону виявлення уздовж стін з вікнами чи дверима.

Для пасивного інфрачервоного сповіщувача як і для будь-якого іншого пристрою виявлення, необхідна деяка ознака (зміна яких-небудь фізичних характеристик чи параметрів об'єкта), що дозволяє прийняти рішення про рух порушника на об'єкті. У даному випадку такою ознакою є зміна інфрачервоного (теплого) випромінювання в контрольованій зоні.

Відомо, що всі тіла з температурою вище абсолютного нуля є джерелами ІЧ-випромінювання. Це відноситься і до людини, різні ділянки тіла якої мають температуру в діапазоні 25-36 °С. Інтенсивність ІЧ-випромінювання буде залежати від багатьох факторів, наприклад, від виду одягу людини. Проте, якщо на об'єкті, що не має джерел ІЧ-випромінювання із змінною температурою, з'являється людина, то буде змінюватися загальний потік ІЧ-випромінювання з контрольованої зони.

Таким чином, ПЧ-сповіщувач повинен реєструвати зміну інфрачервоного випромінювання з появою на об'єкті порушника. У той же час він не повинен реагувати на зміни такого ж випромінювання, викликаного зміною температури фону протягом доби (швидкість зміни температури порядку  $1\text{ }^{\circ}\text{C/хв}$ ), включенням чи відключенням опалювальних приладів, що створюють конвекційні повітряні потоки, тобто сповіщувач повинен бути завадостійким.

Основні елементи, які повинні входити до складу ПЧ-сповіщувача для того, щоб він реєстрував зміну ІЧ-випромінювання, показані на [7] (рис. 2.3).

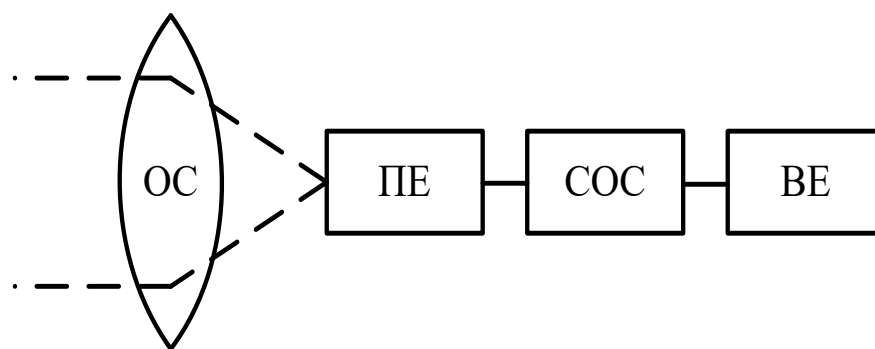


Рис. 2.3 Основні елементи ПЧ сповіщувача

По-перше, це чутливий елемент - піроелемент (ПЕ), що перетворює ІЧ-випромінювання в електричний сигнал. По-друге, оптична система (ОС), яка фокусує на піроелементі ІЧ-випромінювання з визначеної частини об'єкта. По-третє, це схема обробки сигналу (СОС) від чутливого елементу. І, нарешті, виконавчий елемент (ВЕ), що забезпечує підключення сповіщувача до шлейфу сигналізації, тобто сполучення сповіщувача з іншими елементами системи сигналізації.

Піроелемент здійснює перетворення ІЧ-випромінювання з контрольованої зони об'єкта в електричний сигнал, необхідний для схеми обробки. Конфігурація контрольованої зони визначається оптичною системою, що створює визначену діаграму спрямованості сповіщувача і, отже, формує зону виявлення сповіщувача. Схема обробки реалізує визначений алгоритм аналізу вихідного сигналу ПЕ та приймає рішення про наявність чи відсутність руху на

об'єкті. У випадку прийняття рішення про наявність руху, тобто про проникнення на об'єк, активізується виконавчий елемент. Зазвичай, останній елемент – це реле з контактами, які вмикаються в шлейф сигналізації.

Перетворення ІЧ-випромінювання в електричний сигнал здійснює піроприймач. Перші пристрої подібного типу склалися з двох одноплощинних ПЕ, що включалися паралельно. У цьому випадку, якщо ІЧ-випромінювання, що падає на обидва ПЕ, однакові, струм, формований ними, однаковий за величиною і протилежний за напрямком. Отже, вхідний сигнал підсилювача, що впливає з вищесказаного, дорівнює нулю. При несиметричному опроміненні піроелементів їхні сигнали будуть відрізнятися і з'явиться струм на вході підсилювача схеми обробки.

Одна з основних характеристик сповіщувача - це зона виявлення. Зона виявлення – це зона, у якій сповіщувач видає повідомлення про тривогу при переміщенні стандартної цілі (людини) на постійній відстані від сповіщувача. Зона виявлення складається з елементарних чутливих зон - зон оптичної діаграми спрямованості сповіщувача, у яких він реагує на ІЧ-випромінювання. Форма і параметри зони виявлення, як і кількість, розташування і параметри елементарних чутливих зон, у значній мірі визначають чутливість сповіщувача.

Приклад типової реальної діаграми спрямованості приведений на (рис. 2.4) вид зверху (рис. 2.4 а), та вид збоку (рис. 2.4 б). Діаграма спрямованості такого типу називається “широкий кут” чи “об’ємна”.

Це одна з найбільш розповсюджених діаграм спрямованості, що дозволяє контролювати весь об’єм приміщення. Діаграми такого типу можуть відрізнятися декількома основними особливостями. По-перше, наявністю чи відсутністю зони контролю безпосередньо знизу під сповіщувачем. По-друге, співвідношенням чутливості при русі в центрі діаграми і по її краях.

Зауважимо, що рівномірна чутливість по всій діаграмі спрямованості дуже важливий фактор, яким володіють деякі пристрої. Тільки при рівномірній чутливості по всій зоні виявлення можна досягти високої імовірності виявлення при низькому рівні помилкових тривог.

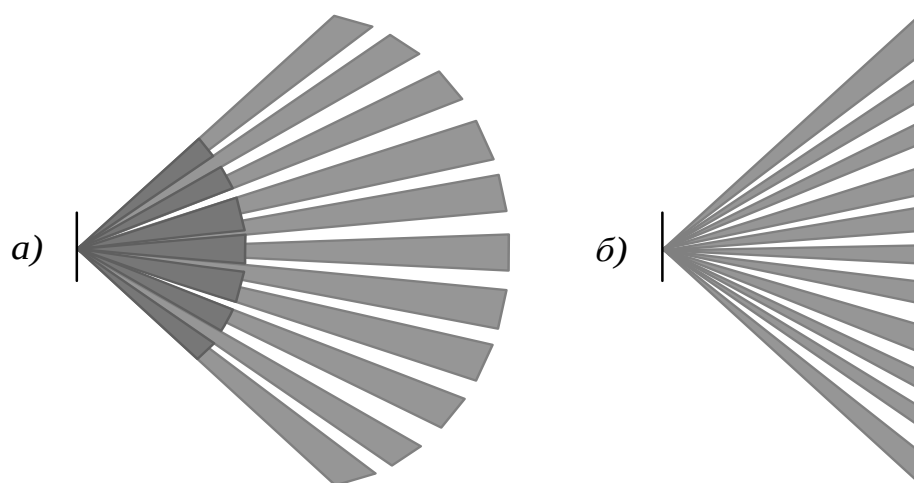


Рис. 2.4 Об'ємна діаграма спрямованості

Інший розповсюджений тип діаграм забезпечує контроль вузької смуги, наприклад, коридору. Така діаграма має на виді зверху два-три промені. Кількість променів на виді збоку (у вертикальній площині) може трохи відрізнятися. Справа в тому, що існують дві схожі діаграми – «коридорна» чи «лінійна» (рис. 2.5) і «вертикальна» чи «бар'єр вертикальна фіранка» (рис. 2.6).

Якщо перша орієнтована в більшій мірі на однакову надійність виявлення при русі як уздовж, так і поперек діаграми, то друга насамперед забезпечує реєстрацію руху поперек, мінімізуючи "вікна" у діаграмі.

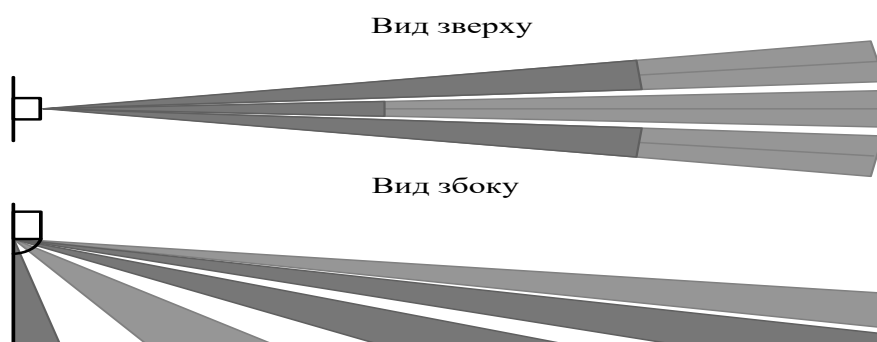


Рис. 2.5 Коридорна діаграма спрямованості

Ще одна особливість пов'язана з необхідністю виключити зону контролю під сповіщувачем. Пояснюється це тим, що ця зона й інша частина діаграми формуються звичайно різними оптичними системами.



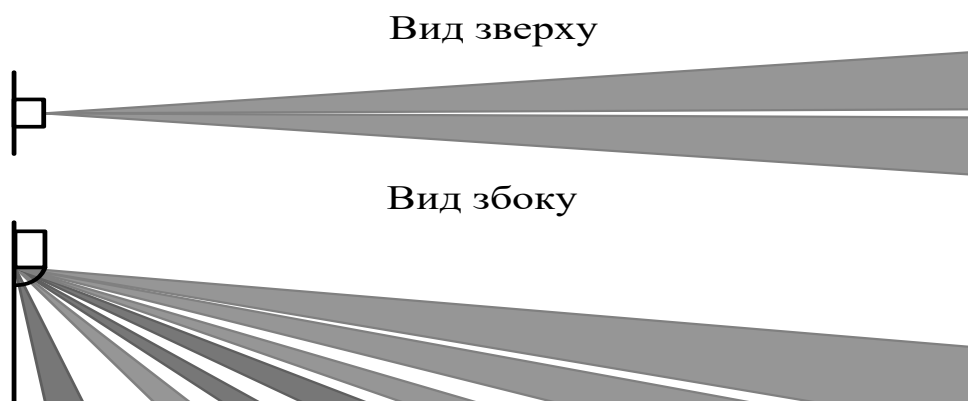


Рис. 2.6 Діаграма спрямованості “вертикальна штора”

Стандартні діаграми спрямованості можуть коректуватися шляхом заклеювання окремих сегментів чи дзеркал лінз Френеля. При цьому з діаграм виявлення виключаються окремі пелюстки.

На (рис. 2.7) наведено приклад пасивних інфрачервоних сповіщувачі [8].



Рис. 2.7 Пасивні інфрачервоні засоби виявлення

#### Магнітоконттактний сповіщувач

Магнітоконттактний сповіщувач містить у собі два основних елементи. Перший елемент – це геркон, що складається з герметичної колби, у якій знаходяться пластини з контактами, які мають малий опір, другий елемент –

магніт [8]. До пластин під'єднані провідники, що забезпечують підключення МКС. Для виготовлення пластин використовуються метали або сплави (наприклад, сталь), які забезпечують ефективне керування пластинами магнітним полем. Один з варіантів побудови геркона – використання протилежно намагнічених пластин. Під впливом магнітного поля від розташованого поруч магніту відбувається замикання чи розмикання контактів. У більшості випадків під впливом магнітного поля контакти нормально замкнуті. При знятті магнітного поля під дією пружних сил відбувається розмикання контактів.

Контакти звичайно покриваються спеціальним сплавом, наприклад, родієвим, що забезпечує малий опір і тривалий термін служби.

На цей час фірми-виробники випускають різноманітні типи МКС, які розрізняються за: способом встановлення, місцем використання, конструктивним виконанням, основними параметрами і іншими ознаками [9] (рис. 2.8).

До основних параметрів магнітоконтактних сповіщувачів відносять наступні:

- робочий зазор. Цей параметр визначає мінімальну відстань, на якій відбувається замикання контактів геркона. Величина робочого зазору залежить від взаємного розташування геркона і магніта. При зсуві магніта в бік величина зазору зменшується. Деякі МКС мають збільшений робочий зазор, що дає можливість встановлювати їх на конструкції, які мають люфти та збільшені зазори між елементами конструкції, що блокуються.

- кількість спрацьовувань. Конструктивне виконання сучасних МКС забезпечує до  $10^7$  спрацьовувань контактів. Це гарантує практично необмежене за часом використання МКС, що перекриває періоди фізичного чи морального старіння інших елементів системи сигналізації. Так, компанія C&K Systems дає довічну гарантію на цей тип пристроїв.

- стійкість до вібрацій і ударних навантажень. Це досить важливий параметр, що впливає на імовірність помилкового спрацьовування. Стійкість до

вібрацій і ударних навантажень пояснюється тим, що при деяких впливах можливі короточасні розмикання контактів.



Рис. 2.8 Магнітоконтатні сповіщувачі

Сповіщувачі розбиття скла.

Акустичні сповіщувачі розбиття скла є найбільш розповсюдженими на цей час. Це викликано рядом їхніх переваг, таких як відсутність якихось елементів на контрольованих поверхнях скла, можливість контролювати кілька вікон одним сповіщувачем та ін. Тому зупинимось докладніше на особливостях акустичних коливань, що виникають при розбитті скла.

Як відомо, при руйнуванні скла виникають акустичні коливання різних частот. У перший момент при ударі по склу воно деформується. Ця деформація, тобто вигин скла, викликає появу акустичних коливань низьких частот. Коли величина деформації досягає граничного значення, відбувається механічне руйнування скла. Останнє супроводжується акустичними коливаннями високих частот. Причому для виявлення факту розбиття скла потрібно враховувати і те, що ці звукові коливання з'являються у визначеному часовому інтервалі [9].

Після удару виникають коливання, спектр яких поширюється до частот близько 25 кГц. При цьому низькочастотні складові зосереджені головним чином в області частот десятків і сотень герц і пов'язані з деформацією скла в момент удару. Ці складові мають максимальну амплітуду в перші 200-300 мс і потім поступово загасають у часі.

Практично відразу після удару виникає широкосмугове коливання, що обумовлене механічним руйнуванням скла. Ці високочастотні складові досить швидко загасають у часі.

Через декілька сот мілісекунд знову виникають високочастотні коливання зі спектральними складовими в області 3-20 кГц. Ці складові викликані акустичними коливаннями, що виникають при падінні осколків скла на підлогу і їхньому подальшому руйнуванні.

У такий спосіб для виявлення факту розбиття скла потрібно реєструвати звукові коливання визначеного спектрального складу і звукові коливання, які з'являються один за одним в деякому часовому інтервалі.

Принцип двоканальної обробки дозволяє істотно зменшити число помилкових спрацьовувань у порівнянні з одноканальним, котрий може бути викликаний звуковими коливаннями іншого походження. Наприклад, падіння зв'язки ключів викликає тільки високочастотні звукові коливання, що не приводять до спрацьовування сповіщувача. Важливо відзначити, що наявність яскраво вираженої низькочастотної складової обумовлена насамперед умовою необхідності виявлення розбиваття скла, закріпленого в рамі. Тобто реальних будівельних елементів.

На (рис. 2.9) зображена структурна схема сповіщувача розбиття скла, що реалізує розглянутий вище алгоритм. Сповіщувач містить у собі [10]:

- мікрофон (М);
- канал, що реєструє низькочастотні коливання, які відповідають деформації (вигину) скла. Канал складається з фільтра низьких частот (ФНЧ), порогового пристрою (ПП1) і одинібратора (ОВ);
- канал, що реєструє високочастотні коливання, які виникають при руйнуванні скла. Канал складається з фільтра високих частот (ФВЧ), детектора (Д) і порогового пристрою (ПП2);
- схему співпадання "І";
- схему фіксації (СФ), що забезпечує або включення реле на визначений час, або фіксацію реле (пам'ять тривоги);

- виконавчий елемент реле «тривога» Р.

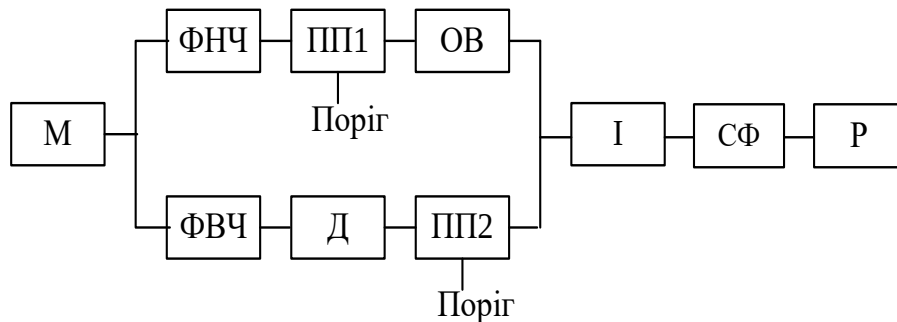


Рис. 2.9 Структурна схема сучасного сповіщувача розбиття скла

Якщо високочастотні акустичні коливання надходять після впливу низькочастотних із затримкою, яка не перевищує тривалість імпульсу одновібратора, то сигнал ОВ відкриває канал «ЗВУК», встановлюючи в робочий стан пороговий пристрій ПП2. Таким чином, якщо за сигналом, що відповідає вигину, з'являються високочастотні коливання, обумовлені руйнуванням скла, вони будуть оброблятися каналом «ЗВУК» і на схему «І» надходять одночасно сигнали з виходів обох каналів. Вихідний сигнал схеми «І», в свою чергу, через схему фіксації включає реле «тривога».

Деякі сповіщувачі розбиття скла різного типу можуть мати відмінності й особливості, наприклад два мікрофони, окремі для кожного каналу.

На (рис. 2.10) зображені сповіщувачі розбиття скла [11].



Рис. 2.10 Сповіщувачі розбиття скла

Комбінований інфрачервоний сповіщувач руху та розбиття скла.

Комбінований сповіщувач руху та розбиття скла призначений для відстеження руху людини в приміщенні, що охороняється і детектування ударів по склу та розбиття скла. Принцип дії сенсора руху заснований на визначенні інфрачервоного (ІЧ) випромінювання. Кожна жива істота - джерело ІЧ випромінювання. Як тільки сповіщувач починає ІЧ-випромінювання в межах охоронної зони, він відсилає сигнал тривоги на центральний блок охоронної сигналізації. У датчику реалізований імунітет від тварин вагою до 25 кг і висотою до 1 м, спрацювання генерується тільки при русі людини. Якщо в приміщенні впаде який-небудь предмет, пробіжить кішка сповіщувач не спрацює.

Вбудований електретний мікрофон дозволяє виявити удари по склу та розбиття скла. При цьому використовується захист від помилкових спрацювань. Вхідний звук аналізується поетапно. Для включення тривоги спочатку повинні бути зроблені низькочастотні звуки (удар по склу), а потім - високочастотні (звук скла, що розбивається), тільки після цього відправиться сигнал тривоги.

Комбінований сповіщувач руху та розбиття скла використовується для охорони практично багатьох об'єктів. Це один з найпоширеніших елементів охоронних сигналізацій що використовуються у приміщеннях (рис. 2.11) [12].



Рис. 2.11 Комбінований сповіщувач руху та розбиття скла

## 2.4 Технічні засоби контролю стану периметрів об'єктів

Активні інфрачервоні засоби виявлення.

Принцип дії активного інфрачервоного сповіщувача полягає в створенні променевого бар'єра, при перериванні якого активний ІЧС виробляє сигнал тривоги.

Активний ІЧС складається з двох технологічно закінчених одиниць: передавача і приймача. Передавач генерує сигнал, спектр якого розташований в інфрачервоному діапазоні. Сигнал передавача приймається приймачем – ІЧС знаходиться в режимі чекання. Якщо ж в режимі очікування сигнал від передавача зникає (на прямій між передавачем і приймачем з'явився об'єкт, що екранує сигнал), то активний ІЧС виробляє сигнал тривоги.

Оптична система джерела випромінювання створює вузькоспрямований промінь ІЧ-випромінювання. У чкості джерела ІЧ-випромінювання використовують напівпровідникові випромінюючі діоди які розташовують у фокусі оптичної системи

ІЧ-випромінювання фокусується оптичною системою ПРМ на чутливий майданчик фотоприймачів (фотодіодів). Отримувані з них імпульси фотоструму посилюються і поступають на пристрої обробки для формування сигналів тривоги.

На (рис. 2.12) наведено зовнішній вигляд активної інфрачервоної системи виявлення порушників [13].

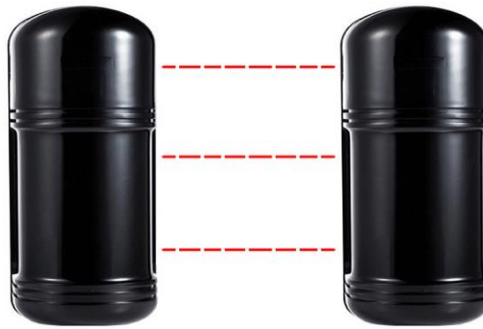


Рис. 2.12 Інфрачервоний бар'єр

#### Сейсмічні засоби виявлення

В даний час при організації охорони території, разом з іншими типами засобів виявлення, достатньо широко застосовуються сейсмічні засоби виявлення, в яких реєструються і потім обробляються сигнали, що виникають в ґрунті (або іншій підстилаючій поверхні) при перетині людиною зони, що охороняється [13].

До основних переваг СЗВ відносяться відсутність власного випромінювання, можливість повного усунення демаскуючих ознак на ділянці, що охороняється, за рахунок установки лінійної частини (чутливих елементів і сполучних кабелів) в ґрунт. Сейсмічні засоби виявлення, будучи пасивними засобами охорони, не виявляються електронними засобами розвідки. Візуально приховані СЗВ різко знижує вірогідність їх подолання навіть при обізнаності порушника про принципи роботи і ТТХ засобу. Сейсмічні засоби зручні для блокування ділянок на нерівній місцевості і широко застосовуються в цілях охорони протяжних рубежів держкордону і периметрів об'єктів .

До недоліків СЗВ відносяться низька перешкодостійкість при заданій вірогідності виявлення ( $P_{\text{виявл}} > 0,9 \dots 0,95$ ) в умовах дії різноманітних сейсмічних перешкод (наприклад, від літаків, автотранспорту, промислових підприємств, дощу, вітру і тому подібне).



Низька перешкодостійкість обмежує тактичні можливості сейсмічних засобів. Проте, не дивлячись на це і враховуючи вищезазначені переваги СЗВ, на сьогоднішній день зберігається інтерес різних служб охорони, а також розробників техніки сигналізації до ЗВ даного типу.

Принцип дії сейсмічних засобів охорони заснований на реєстрації (виявленні) коливань, що виникають в ґрунті при переміщенні людини по поверхні землі. Чутливі елементи, встановлені в поверхневому шарі ґрунту на глибині 20...50 см, перетворюють сейсмічні коливання в електричні сигнали, що поступають на вхід ЗВ. Ділянка місцевості, подолання якої має бути виявлене сейсмічним засобом, називається зоною виявлення. СЗВ можна умовно розділити на два класи: для блокування малих ділянок місцевості і для охорони протяжних рубежів. Виходячи з особливостей вирішуваних тактичних завдань, перші зазвичай мають ЗВ близьку по формі до круга, радіус якого не перевищує 3...5 м. Протяжність зони виявлення СЗВ другого класу знаходиться в межах від 10 до 100 м, а ширина – від 5 до 20 м.

У якості чутливих елементів, призначених для перетворення механічної енергії сейсмічних коливань в електричний сигнал, можуть бути використані:

- точкові чутливі елементи (сейсмоприймачі);
- протяжні чутливі елементи.

Найпоширенішим типом точкового чутливого елементу є сейсмоприймач електродинамічного типу [14] (рис. 2.13). Конструкція їх вдає із себе герметичний корпус, усередині якого знаходиться магнітна система. У зазорі магнітної системи вільно переміщається котушка індуктивності, підвішена на гнучких підвісах. Електричні сигнали, що виникають при русі котушки, поступає на зовнішні виводи.

В якості протяжного чутливого елемента, як правило, використовується лінія, утворена ланцюжком послідовно сполучених електродинамічних сейсмоприймачів.

На виході такої лінії відбувається підсумовування сигналів від окремих СП. Типова кількість СП в лінії – 10 ... 20 м, відстань між СП – 5 ... 10 м.



Рис. 2.13 Чутливий елемент електродинамічного типу

Також у якості чутливих елементів використовуються протяжні чутливі елементи – трибокабелі, еластичні труби з рідиною, сполучені з датчиками тиску [15]. Трибоелектричний вібраційний кабель перетворює механічні коливання інженерних загороджень (на якому він закріплений) в електроімпульси. В результаті мікродеформацій у структурі кабельного сенсора (утвореної центральним провідником, його діелектриком і проводить опліткою), створюється внутрішня електризація, що викликає різницю потенціалів між провідниками, що отримала назву трибоефект або контактна електризація. Кабель, що працює на трибоефекті, вимагає використання його на загородженнях які володіють видимою гнучкістю, в момент його подолання порушником. До таких загороджень відносяться сітка «рабиця», зварена решітка з прутком до 6 мм, колючий дріт, армована колючий дріт.

Радіопроменеві сповіщувачі.

Пристрій забезпечує сигнальне блокування об'єктів, що охороняються, при вторгненні сторонніх осіб на протяжних ділянках периметра до 500 м відкритій місцевості і в умовах міської забудови, протяжністю до 100 м Пристрій реєструє внесення тілом людини змін у мікрохвильове електромагнітне поле, що посиляється спрямованими антенами від передавача до приймача [15].

На рис. 2.14 показано приклад двопозиційної радіо променевої системи та її зони виявлення.

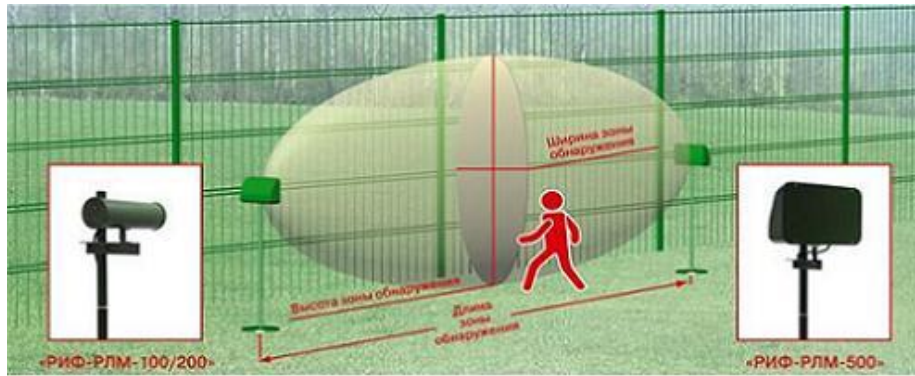


Рис. 2.14 Зона виявлення радіопроменевої системи

Засіб відноситься до галузі охоронної сигналізації і хвильової техніки НВЧ, зокрема, до пристроїв і способів для формування радіопроменевої зони між рознесеними в просторі передавачем і приймачем НВЧ для виявлення людини, яка вторгається у цю зону. Радіопроменеві сповіщувачі (системи, сенсори, датчики) широко відомі в техніці охорони [16]. Зону виявлення формують за допомогою антен, встановлених на протилежних сторонах охороняемого кордону і які спрямовуються зустрічно максимумами діаграм спрямованості.

Від місця установки антени до місця торкання радіолучом ґрунту існує "мертва зона" по виявленню. Відомий недолік усувають шляхом збільшення до 1,0-1,5 м вертикального розміру апертури антени і установкою нижнього краю апертури над рівнем ґрунту. При цьому багаторазово зростає відношення корисний сигнал/завада, зникають "мертві зони".

Радіопроменеві однопозиційні сповіщувачі (рис. 2.15) працюють на ефекті Доплера. У основу роботи датчика закладено ефект Доплера – зміна частоти відбитої хвилі, внаслідок руху випромінювача, приймача чи відбивача. У даному модулі частота радіохвилі, що випромінюється ним, змінюється внаслідок руху відбивача (перешкоди). При наближенні об'єкта частота відбитого сигналу збільшується, а видаленні - зменшується. При нерухомому об'єкті частота, що випромінюється і приймається, рівні.

Переваги таких систем:

- безконтактне виявлення об'єктів;
- мала чутливість до параметрів довкілля (температура, вологість, шум, пил, світло тощо);
- максимальна дальність виявлення до 20 метрів;
- мізерна випромінювана потужність.

Типові характеристик передавача:

Характеристики передавача:

- частота передачі: 10.525 ГГц;
- точність встановлення частоти: 3МГц;
- вихідна потужність: 13dBm EIRP;
- споживаний струм: 60mA макс. 37mA;
- випромінєні гармоніки: <-10dBm;



Рис. 2.15 Радіопроменевий однопозиційний сповіщувач

## 2.5 Засоби прийому та обробки сигналів сповіщувачів

Прилади приймально-контрольні (контрольні панелі) відносяться до технічних засобів контролю і реєстрації інформації [19]. Вони призначені для безперервного збору інформації від сповіщувачів, включених в шлейф сигналізації, аналізу тривожної ситуації на об'єкті, формування та передачі сповіщень про стан об'єкта на пульт централізованого спостереження, а також управління місцевими світловими і звуковими сповіщувачами і індикаторами.

Крім того, прилади забезпечують здачу і зняття об'єкта з охорони за прийнятою тактикою, а в ряді випадків - електроживлення сповіщувачів. Прилади є основними елементами, що формують на об'єкті інформаційно-аналітичну систему охоронної або охоронно-пожежної сигналізації. Така система може бути автономною або централізованою. При автономній охорони прилади встановлюються в приміщенні (пункті) охорони, який розміщується на об'єкті або в безпосередній близькості від нього. При централізованій охороні об'єктовий комплекс технічних засобів, що формується одним або декількома приладами, утворює об'єктову підсистему охоронно-пожежної сигналізації, яка за допомогою системи передачі сповіщень передає в заданому вигляді інформацію про стан об'єкта на пульт централізованого спостереження, що розміщується в центрі прийому сповіщень про тривогу (пункті централізованої охорони). Інформація, яка формується приладом, як при автономній, так і централізованої охорони передається співробітникам спеціальних служб забезпечення охорони об'єкта, на яких покладено функції реагування на тривожні повідомлення, що надходять з об'єкта.

З метою підвищення достовірності одержуваної інформації при організації контролю стану об'єкта за допомогою технічних засобів застосовують багаторубежіві комплекси охоронної сигналізації. Кожен з рубежів сигналізації являє собою сукупність послідовно об'єднаних електричним колом (шлейфом сигналізації) спільно діючих технічних засобів охоронної сигналізації, що дозволяє видати повідомлення про проникнення (спробі проникнення) в зону, що охороняється (зони) незалежно від інших технічних засобів, який не входять в даний ланцюг. При цьому в кожен рубіж сигналізації включають сповіщувачі, засновані на різних принципах дії.

Крім здачі під охорону і зняття об'єкта (приміщення) з охорони за прийнятою тактикою, зазвичай забезпечують електроживлення сповіщувачів.

Прилади приймально-контрольні класифікуються за:

- інформаційної ємності (кількість контрольованих шлейфом сигналізації) на прилади малої (до 5 ШС), середньої (від 6 до 50 ШС) і великої (понад 50 ШС) інформаційної ємності;
- інформативності - можуть бути малої (до 2 видів повідомлень), середньої (3 ... 5 видів) і великої (понад 5 видів) інформативності.

За кількістю напрямків передачі інформації вони поділяються на системи з одно- і двобічної передачею інформації (з наявністю зворотного каналу).

За способом відображення надходить на пульт централізованого спостереження інформації системи передачі сповіщень підрозділяються на системи з індивідуальним або груповим відображенням інформації у вигляді світлових і звукових сигналів, з відображенням інформації на дисплеї з застосуванням пристроїв обробки та накопичення бази даних.

Шлейф сигналізації - це електричний ланцюг, що з'єднує вихідні ланцюги сповіщувачів, що включає в себе допоміжні елементи (діоди, резистори і т.п.), з'єднувальні дроти і коробки та призначена для видачі сповіщень про проникнення, спробу проникнення, пожежі, несправності, а в деяких випадках і для подачі електроживлення на сповіщувачі. Таким чином, шлейф сигналізації призначений для контролю стану деякої зони, що охороняється.

Зона охорони - це частина об'єкту, що охороняється, контрольована одним або декількома шлейфами сигналізації.

Сучасні багатофункціональні КП мають широкі можливості по організації систем охоронної, пожежної та охоронно-пожежної сигналізації. Знання цих можливостей дозволить зробити правильний вибір КП, характеристики і параметри якої найбільш повно задовольняють вирішення поставлених завдань з охорони конкретного об'єкта.

Робота КП може здійснюватися в різних режимах, а саме: охорона, спостереження (зняття з охорони), програмування.

Режим "охорона".

У цьому режимі КП контролює свої параметри і стан шлейфів. Порухення шлейфів призводить до формування сигналів тривоги. При цьому можливі наступні різновиди режиму:

- повна охорона - КП контролює стан всіх шлейфів і самого себе.
- часткова охорона з контролем частини шлейфів і самій КП.

Процедура взяття об'єкта під охорону і зняття з охорони відноситься до тактичних параметрах і може розділятися на такі різновиди:

- автоматична постановка під охорону.
- постановка на охорону з затримкою на вихід.
- постановка на охорону без затримки на вихід.

Режим "спостереження (знято з охорони)"

У режимі «спостереження» КП знятий з охорони, але продовжує контролювати всі шлейфи і самого себе.

Шлейф сигналізації є однією з необхідних складових частин технічної системи охорони. Практика показує, що однією з основних причин нестійкої роботи приладів ТСО на об'єкті є порушення шлейфу сигналізації, які представляють собою відмову у вигляді обриву або короткого замикання в шлейфі. Не повинна виключатися також можливість умисного втручання в електричний ланцюг шлейфу з метою порушення його правильного функціонування (саботаж) [17].

Прилади й пульти приймально-контрольні пожежні призначені для живлення пожежних сповіщувачів по шлейфах пожежної сигналізації, прийому тривожних сповіщень від пожежних сповіщувачів, контролю пожежних шлейфів на обрив і коротке замикання, формування повідомлень «Пожежа» і «Несправність», формування сигналів включення систем пожежогасіння та димовидалення, а також для передачі цих повідомлень на пульт централізованого спостереження або інші ППК.

Основними характеристиками пожежних ППК, також як і охоронних, є інформаційна ємність і інформативність.

Сигнально-пускові пристрої - це, по суті, ті ж прилади приймально-контрольні, які доповнені можливістю формування сповіщення «Увага» при спрацьовуванні одного пожежного сповіщувача, сповіщення «Пожежа» при спрацьовуванні не менше двох пожежних сповіщувачів, регульованою затримкою сигналу пуску систем пожежогасіння, можливістю управління системами оповіщення про пожежу. Відмінною особливістю ППК даного покоління приладів є променева структура побудови систем пожежної сигналізації та використання неадресних, порогових пожежних сповіщувачів, які самі приймають рішення про пожежу, як тільки контрольований ними параметр виходить за рамки допустимого значення.

Виносний пристрій оптичної сигналізації (ВПОС) призначений для дублювання оптичного сигналу спрацьовування пожежних сповіщувачів, візуальний оперативний доступ до яких утруднений. ВПОС рекомендується використовувати для визначення сповіщувача, який подав повідомлення «Пожежа», і встановлювати в доступному для огляду місці, наприклад в коридорі над дверима приміщення, що охороняється.

Системи пожежної сигналізації діляться на три класи: неадресні системи, адресні і адресно-аналогові пожежні системи.

Головна їхня відмінність це метод, за яким система приймає рішення про тривожну ситуацію, тобто про пожежу. У неадресних і адресних системах це рішення приймається безпосередньо самими встановленими пожежними сповіщувачами і потім тривожний сигнал передається на приймально-контрольоване обладнання і на підставі цього сигналу з сповіщувача включається система пожежогасіння.

Спроби виявити загоряння на ранній стадії шляхом зниження порогів чутливості точкових димових сповіщувачів зазвичай призводять до помилкових спрацьовувань пожежної сигналізації і хибним пусків систем пожежогасіння. Постійний пошук компромісу між раннім виявленням і хибним пуском.

В адресно-аналогових системах принцип прийняття рішення про виникнення пожежі зовсім інший. На приймально-контрольне обладнання



передається значення контрольованого сповіщувачем параметра (температура, задимленість в приміщенні). Головне обладнання постійно відстежує стан навколишнього середовища в усіх приміщеннях будівлі і відстежує динаміку зміни зазначених параметрів. На підставі цих даних приймає рішення не тільки про формування сигналу «Пожежа», а й сигналу «Попередження». Тобто адресно-аналогова система пожежної сигналізації побудована на ухваленні рішення про тривогу не окремими пожежними датчиками, а приймально-контрольним обладнанням на основі динаміки зміни даних, що надходять з сповіщувачів. Адресно-аналогові системи, постійно контролюючи стан середовища в приміщенні, негайно виявляють зміну температури або задимленість і видають черговому попереджуючий сигнал.

Раннє виявлення спалаху дозволяє своєчасно евакуювати людей ще на початковій стадії пожежі і провести запуск автоматичної установки пожежогасіння. Попутно вирішується так само ряд важливих завдань, наприклад, контроль працездатності сповіщувачів. Так, в адресно-аналоговій системі в принципі не може бути несправного сповіщувача, що не виявленого приймально-контрольним приладом, так як весь час сповіщувач повинен передавати певний сигнал. Якщо до цього додати потужну самодіагностику самих сповіщувачів, автоматичну компенсацію запиленості та виявлення запилених димових сповіщувачів, то стає очевидним, що ці чинники тільки підвищують ефективність адресно-аналогових систем.

Конструктивно прилади приймально-контрольні можуть бути виконані як однопозиційні (одноблокові) і багатопозиційні (багатоблокові) (рис. 2.16). Незважаючи на істотні відмінності в тактико-технічних характеристиках сучасні прилади мають багато спільного в конструктивному виконанні. У сучасних приладах широко застосовуються цифрові методи обробки сигналів. Перетворення за допомогою аналогово-цифрового перетворювача (АЦП) сигналу, що знімається з виходу шлейфа сигналізації у кодований імпульсний сигнал розширює можливості його обробки, підвищує точність, так як послідовні перетворення інформації в цифровій формі не приводять до зменшення похибок,

а при обробці аналогових сигналів похибки збільшуються на кожному етапі перетворення.



Рис. 2.16 Прилад прийомо-контрольний охоронно-пожежний

Висновки до другого розділу.

Встановлено, що існують радіальна, шлейфова та деревовидна структури побудови сучасних комплексів технічних систем охорони.

До складу засобів, що використовуються у технічних системах охорони входять сповіщувачі – засоби виявлення різного фізичного принципу дії, прилад прийомо-контрольний охоронно-пожежний, лінії сполучення між ними – шлейфи..

Для охорони внутрішніх рубежів об'єктів найчастіше використовуються пасивні інфрачервоні засоби виявлення, магнітоконтатні сповіщувачі, сповіщувачі розбиття скла, комбінований інфрачервоний сповіщувач руху та розбиття скла.

Для охорони зовнішніх рубежів об'єктів найчастіше використовуються активні інфрачервоні засоби виявлення, сейсмічні засоби виявлення, ємнісні сповіщувачі, радіопроменеві сповіщувачі.

### Розділ 3.

## ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ

Для розробки технології захисту інформації від витоку матеріально-речовим каналом необхідно розглянути основні принципи побудови системи безпеки.

Принципи побудови системи безпеки.

**Законність.** Заходи щодо забезпечення безпеки ресурсів підприємства будуються виходячи з чинних законів, правової та нормативно-методичної бази. Вся робота проводиться за суворого дотримання прав людини, законних інтересів учасників господарської діяльності, держави.

**Достатність та економічна доцільність.** Захист повинен будуватися із забезпеченням оптимальної відповідності критеріїв «достатність – ефективність – вартість», тобто при заданій та досяганій ефективності мінімально можливі витрати на заходи захисту.

**Комплексність та індивідуальність.** Побудова системи безпеки має ґрунтуватися на врахуванні всіх можливих (у тому числі специфічних) загроз ресурсам саме даного підприємства. При цьому слід враховувати, що:

- невідомо, ким, коли, де і як може бути порушена безпека об'єкта, оскільки має місце наявність «людського чинника» (принцип невизначеності);
- з принципу невизначеності та обмеженості ресурсів засобів захисту впливає неможливість створення ідеальної системи захисту;
- виходячи з неможливості створення ідеальної системи захисту, слід вибирати той чи інший ступінь ризику (принцип мінімальної шкоди) з урахуванням особливостей загроз безпеці та конкретних умов об'єкта (принцип мінімального ризику);
- внаслідок невизначеності процесу захисту захисні заходи мають плануватись проти всіх форм загроз – принцип «захист усіх від усіх».

**Безпека часу.** При створенні системи передбачається враховувати два фактори часу: абсолютний час, протягом якого необхідне збереження безпеки об'єктів захисту, та відносний час, тобто проміжок часу від моменту виявлення зловмисних дій щодо СЗ до досягнення зловмисником своєї мети.

**Персональна відповідальність.** Організація захисту об'єкта повинна передбачати персональну відповідальність кожного співробітника за збереження режиму безпеки в межах своїх повноважень або відповідних інструкцій, а також обмеження доступу до цінностей, що захищаються, без необхідності використання їх для виконання посадових обов'язків.

**Взаємодія та співпраця служб та персоналу.** Заходи щодо безпеки вимагають координації діяльності всіх підрозділів підприємства. При цьому має бути передбачено створення сприятливої внутрішньої та зовнішньої атмосфери безпеки (довірчі відносини між співробітниками служби безпеки та персоналом). За певними напрямками забезпечення безпеки організується співпраця з усіма зацікавленими організаціями та особами, зокрема з правоохоронними та іншими органами держави.

**Захист засобів забезпечення захисту.** Будь-який захисний захід або засіб має, у свою чергу, бути захищеним.

Вибір варіанта охорони об'єкта слід розпочинати з визначення його важливості, кількості приміщень, що підлягають охороні, характеру та структури розміщення цінностей. Спочатку проводиться аналіз основних уразливих місць за периметром об'єкта: вікон, дверей, підлог. Не рідкісні випадки проникнення на об'єкти через стелю та некапітальні стіни. Зазначені вразливі місця обладнуються охоронною сигналізацією. На важливих об'єктах ряд приміщень оснащуються додатковими рубежами сигналізації. Вони підключаються лініями міських телефонних станцій (ГТС) на окремі номери системи передачі сповіщень (СП), а за їх відсутності на окремі номери ПКП.

На промислових підприємствах, базах, складах, установах банків та інших об'єктах інформаційної діяльності необхідно створювати зовнішній рубіж

сигналізації за периметром огороження. Варіанти охорони об'єктів повинні вибиратися за такою методикою:

**Перший етап.** Визначення характеристики об'єкта.

1. Тип об'єкта та його важливість чи цінність, характер наявних цінностей, місце їх розташування та концентрація.

2. Структура об'єкта:

- кількість приміщень, типи та розміри, розташування;
- кількість вразливих місць, їх конструктивні особливості та розміри.

3. Телефонізація та характеристика мережі живлення.

**Другий етап.** Визначення тактики охорони.

1. Вибір виду сигналізації (автономна чи централізована).

2. Вибір структури охорони (кількість рубежів сигналізації на об'єкті та кількість пультових номерів).

3. Визначення можливих варіантів живлення апаратури (від мережі чи джерел резервного питания).

4. Визначення структури та значущості рубежів сигналізації:

- визначення кількості охоронних та пожежних шлейфів;
- поділ охоронних і пожежних шлейфів на самостійні ділянки, що блокуються, визначення ділянок, що блокуються;
- визначення способу блокування вразливих ділянок (відкриття, пролом, комбінація та інші способи: обсяг, зона, пастка);
- розміри ділянок, що блокуються.

5. Вибір технічних засобів виявлення:

- контрольованої ознаки (точковий, лінійний, поверхневий, об'ємний);
- способу виявлення (магнітоконттактний, ударноконттактний, п'єзоелектричний, ємнісний, радіохвильовий, ультразвуковий, оптико-електронний, комбінований);
- співісшувачів з конкретними тактико-технічними характеристиками (надійність, складність установки та монтажу, зручність ТО та ремонту, маскуючі засоби).

#### 6. Вибір типу приймально-контрольних приладів:

- тип ППК (ємність, складність монтажу, зручність ТО та ремонту);
- елементів індикації, контролю та сигналізації порушення;
- визначення та реалізації порядку погодження із СП;
- визначення структури розміщення ППК, кінцевого пристрою, джерел живлення (основного та резервного).

При обладнанні об'єктів із підключенням встановлених на них засобів сигналізації на ПЦН пожежні та охоронні шлейфи повинні бути розділені, мати самостійні ПКП та пультові номери. За наявності на об'єкті постів охорони реалізація роздільної структури вирішується установкою ВКП із підключенням пожежних та охоронних шлейфів на окремі номери.

Слід зазначити, що усталена система забезпечення охорони об'єктів, має деякі недоліки:

1. Як правило, організована система охоронної сигналізації включає лише внутрішні технічні засоби охорони, без додаткового блокування периметра об'єкта (периметральна сигналізація, відеоспостереження (СВН), контроль доступу).

2. Внаслідок відсутності раннього сповіщення про проникнення на територію об'єкта, фактичне проникнення злочинця всередину приміщення має обмежений інтервал часу, що навіть за хорошої організації реагування підрозділів забезпечення безпеки, як правило, не може забезпечити затримання злочинців.

3. Типізація блокування об'єктів засобами охоронної сигналізації призводить до вироблення стійких методик цілеспрямованого порушення стійкості функціонування охоронної сигналізації об'єкта, а отже, зниження ефективності забезпечення захисту.

4. Як істотний недолік слід наголосити на наявності єдиного алгоритму організації службового інформаційного сигналу (СІС) та алгоритму кодування СІС при забезпеченні охорони об'єктів різної категорії важливості.

Виходячи із положень усталеної методики та враховуючи вищеперераховані недоліки розроблено технологію захисту захисту інформації від витоку матеріально-речовим каналом.

**Перший етап.** Визначення характеристики об'єкта інформаційної діяльності.

1. Категорія об'єкту інформаційної діяльності. В межах цього ОІД характер конкретних об'єктів захисту, місця їх розташування, концентрація.

2. Структура ОІД:

- кількість приміщень, розміри, розташування;
- вразливі місця, їх конструктивні особливості та розміри.

3. Характеристика мережі електроживлення.

**Другий етап.** Визначення тактики охорони ОІД.

1. Вибір виду охоронної системи (автономна чи централізована).

2. Визначення можливих варіантів електроживлення апаратури (централізована мережа, джерела резервного питания).

3. Визначення структури та важливості рубежів сигналізації:

- визначення кількості охоронних та пожежних шлейфів;
- визначення способу блокування вразливих ділянок (відкриття, пролом, розбиття вікна, комбінація та інші способи: обсяг, зона);
- розміри ділянок, що блокуються.

4. Вибір технічних засобів виявлення:

- контрольованої ознаки (точковий, лінійний, поверхневий, об'ємний);
- способу виявлення (магнітоконттактний, п'єзоелектричний, ємнісний, активний інфрачервоний, радіохвильовий, ультразвуковий, оптико-електронний, комбінований);
- сповіщувачів з конкретними тактико-технічними характеристиками (надійність, складність установки та монтажу, зручність ТО та ремонту, маскуєчі засоби).

5. Вибір типу приймально-контрольних приладів:

- тип ППК (ємність, адресний або неадресний, складність монтажу, зручність ТО та ремонту);
- елементів індикації, контролю та сигналізації порушення;
- визначення та реалізації порядку погодження із засобами передачі інформації (для централізованих систем).

При обладнанні об'єктів із підключенням встановлених на них засобів сигналізації на пульт централізованого спостереження, пожежні та охоронні шлейфи повинні бути розділені, мати самостійні ПКП та пультові номери. За наявності на об'єкті постів охорони реалізація роздільної структури вирішується установкою виносних контрольних панелів із підключенням пожежних та охоронних шлейфів на окремі номери.

Із врахуванням положень даної технології розроблено систему захисту ІзОД від витоку матеріально-речовим каналом (рис. 3.1).

**Перший етап.** Визначення характеристики об'єкта інформаційної діяльності.

1. Об'єкт другої категорії, тобто здійснюється обробка цілком таємної інформації і відповідно до Закону України про Державну таємницю необхідно створювати комплекс технічного захисту інформації від витоку технічними каналами.

2. В приміщенні розташовано три ОІД. Розташовані в одній будівлі, контрольована зона визначається зовнішньою огорожею. Перепускний режим наявний. Вразливі місця – двері, вікна будівлі та зовнішня огорожа.

3. Наявне централізоване енергоживлення.

**Другий етап.** Визначення тактики охорони ОІД.

1. Технічна система охорони – автономна.

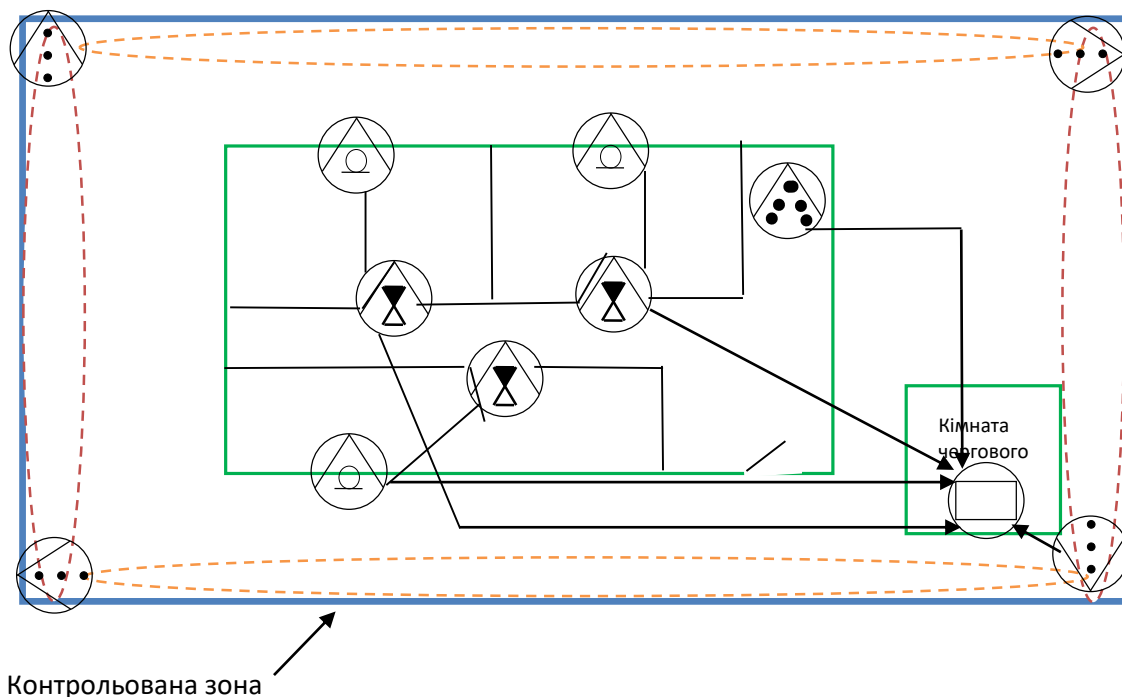
2. Основний варіант електроживлення – централізований. Резервування – за рахунок акумуляторних батарей приладу прийомо-контрольного.

3. З врахуванням необхідності блокування периметру об'єкту для охорони приміщення потрібно п'ять шлейфів. З точки зору блокування ділянок наявні: розбиття вікна, відкриття дверей, фізичний перетин контрольованої зони



об'єкту. Ділянки – периметр об'єкту (контрольована зона), приміщення – кімнати.

4. Для реалізації технології протидії витоку інформації матеріально-речовим каналом необхідно задіяти точкові, об'ємні та лінійні системи.



Прилад приємо-контрольний неадресний;



Інфрачервоний бар'єр;



Магнітоконтатний сповіщувач;



Акустичний розбиття скла;



Пасивний інфрачервоний сповіщувач.

Рис. 3.1 Реалізація технології протидії витоку інформації матеріально-речовим каналом

За способом виявлення це будуть: магнітоконтатні, пасивний інфрачервоний, акустичні розбиття скла та активний інфрачервоний бар'єр.

Конкретні типи систем.

### **Магнітоконтантні.**

Обрано тип Електрон ЕСМК-7П.

Параметри.

Тип монтажу            накладний.

Робочий зазор            18 мм

Зазор відпускання    25 мм

Можливість монтажу на металеві двері    Є.

Робочий струм            100 мА

Умови експлуатації    -30 °С + 60 °С

Саме цей тип сповіщувача обрано тому, що цього можна монтувати на металеві двері. Згідно НД ТЗІ двері режимних об'єктів повинні бути оббиті залізними листами або бути металевими.

### **Інфрачервоний бар'єр.**

Для блокування периметру ОІД (контрольована зона), доцільно використати ІЧ бар'єр Lightwell LBW-100-10. Призначений для зовнішнього застосування.

Параметри.

Тип застосування            зовнішнє;

Кількість ІЧ променів    10;

Робоча температура        -30 +55;

Висота                        172 см

### **Акустичний розбиття скла.**

У якості сповіщувача розбиття скла застосовано сповіщувач типу Slow GBD-2. Він відноситься до двоканальних сповіщувачів і цим досягається малий рівень хибних спрацьовувань. Відомо що процес розбиття скла характеризують дві ознаки. Перша – глухий низькочастотний звук від удару по склу, і друга – через декілька мілісекунд - власне високочастотний звук від руйнування скла. Саме ці дві складові аналізує цей сповіщувач при прийнятті рішення.

Параметри.

|                    |            |
|--------------------|------------|
| Дальність дії      | 10 м;      |
| Кут детектиції     | 170°       |
| Напруга живлення   | 9 – 16 В4  |
| Робоча температура | -20 +50 С° |

#### **Пасивний ІЧ сповіщувач.**

У якості пасивного ІЧ сповіщувача застосовано прилад Bosch ISC-BPR2-WP12. Прилад задовольняє тактичним вимогам застосування та має невелику вартість.

#### **Параметри.**

|                        |                                                   |
|------------------------|---------------------------------------------------|
| Зона виявлення приладу | 12x12 м                                           |
| Тип зони виявлення     | об'ємна;                                          |
| Напруга живлення       | 9-15 В постійного струму, струм споживання 10 мА; |
| Тампер                 | присутен;                                         |
| Робоча температура     | 10°С +50°С.                                       |

#### **Прилад прийомо-контрольний.**

Виходячи з того, що кількість шлейфів ТСО невелика використовується неадресний ППКОП типу Лунь – 9Т. Він задовільняє вимогам технології побудови системи захисту інформації від витоку матеріально-речовим каналом при невеликій власній вартісті.

#### **Параметри.**

|                                         |                                                       |
|-----------------------------------------|-------------------------------------------------------|
| Максимальна кількість охоронних шлейфів | 8;                                                    |
| Живлення приладу                        | мережа 220 В, резервне від власного аккумулятора 12В; |
| Вихід для живлення сповіщувачів         | 12 В;                                                 |
| Вихід струму для сирени                 | 200 мА;                                               |
| Висновок по розділу.                    |                                                       |

Розглянуто загальну концепцію побудови системи захисту об'єкту. Грунтуючись на концепції розроблено технологію захисту інформації від витоку матеріально-речовим каналом.

Приведено практичний приклад застосування розробленої технології на прикладі побудови системи захисту інформації від витоку матеріально-речовим каналом з об'єкту інформаційної діяльності.

## ВИСНОВКИ

У дипломній роботі проаналізовано загрози інформації на об'єкті інформаційної діяльності. Встановлено, що основною загрозою витоку інформації з обмеженим доступом з ОІД матеріально-речовим каналом є крадіжки матеріальних носіїв інформації.

Показано, що ефективним засобом запобігання витоку інформації матеріально-речовим каналом є використання на об'єкті інформаційної діяльності технічної системи охорони.

Встановлено, що технічна система охорони складається зі сповіщувачів, приладу-прийомо-контрольного та фізичного середовища передачі інформації. Для охорони зовнішніх та внутрішніх рубежів лю'єкту захисту доцільно використовувати пасивні інфрачервоні сповіщувачі, сповіщувачі розбиття скла, магнітоконтантні сповіщувачі, активні інфрачервоні сповіщувачі.

Проаналізовано загальні вимоги до системи безпеки об'єкту і на підставі аналізу розроблено технологію захисту інформації від витоку матеріально-речовим каналом з об'єкту інформаційної діяльності.

Показано практичний приклад реалізації розробленої технології.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України Про інформацію № 2657-ХІІ від 2 жовтня 1992 року.
2. Закон України. Про державну таємницю. №1079-ХІV 21 вересня 1999 року.
3. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
3. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
4. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации / Под ред. В.А. Хорошко. – К.: 2010. – Том I.
5. Сучасний стан захисту інформації. – Доступний з [http://www.immsp.kiev.ua/publications/articles/2009/2009\\_2/Litvinov\\_02\\_2009.pdf](http://www.immsp.kiev.ua/publications/articles/2009/2009_2/Litvinov_02_2009.pdf)
6. Системы и устройства информационной безопасности. Учебное пособие / под ред. проф. В.А.Хорошко / Соавторы: А.П.Провозин, О.В.Рыбальский, В.А.Хорошко, Д.В.Чирков. – К.: ДУИКТ, 2007.
7. Технічні засоби охорони об'єктів: Методичні рекомендації до виконання лабораторних робіт / Уклад.: В.В.Литвин, В.О.Темніков. – К.: НАУ, 2014. – 129 с.
8. Методы и средства защиты информации. В 2-х томах / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко, Под ред. В.А.Хорошко. – К.: Арий, 2008.– Том II. Информационная безопасность. – 344 с.
9. Сигналізація. – Доступний з <http://www.znanius.com/3798.html?&L>
10. [http://www.bezpeka-shop.com/catalog/datchiki\\_20467/](http://www.bezpeka-shop.com/catalog/datchiki_20467/)
11. <http://bastion.lviv.ua/ua/shop/category/security/izveshchateli-ohrannye>
12. Електронна книга «Кібервійна та безпека об'єктів критичної інфраструктури». / Юрій Когут. – 2021 – 336 с.
13. Технічний захист інформації. / Богуш В.М., Бровко В.Д., Козюра В.Д., Кобус О.С. – К: Ліра-К, 2023. – 508.

14. Системи охоронної сигналізації. Технічні засоби виявлення. / Ігор Груба – К.: СОЛОН-прес, 2011, 220 с.

15. Барсуков, В.С. Безпека: технології, засоби, послуги / В.С. Барсуков. - К., 2001 - 496 с.

16. Ярочкін, В.І. Інформаційна безпека. Підручник для студентів вузів / 3-є вид. - К.: Академічний проект: Трікста, 2005. - 544 с.

17. Барсуков, В.С. Сучасні технології безпеки / В.С. Барсуков, В.В. Водолазський. - К.: Нолидж, 2000. - 496 с.

## ДОДАТКИ



# **ДОДАТКИ**

Кваліфікаційна робота здобувача освітнього ступеня «МАГІСТР»

## ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ

Спеціальність: 125 – Кібербезпека та захист інформації

Виконав: Антон ІНЮШЕВ

Керівник: к.т.н., доц. Юрій ПЕПА

Київ - 2025

### АКТУАЛЬНІСТЬ РОБОТИ

2

#### Актуальність

- матеріально-речовий канал є одним із шляхів витоку інформації з об'єктів інформаційної діяльності;
- витік матеріальних носіїв, чернеток, бракованої продукції та службових документів може спричинити фінансові й репутаційні втрати;
- технічна система охорони розглядається як інструмент протидії несанкціонованому винесенню матеріальних носіїв інформації.

Мета роботи:  
підвищити ефективність захисту  
інформації від витоку  
матеріально-речовим каналом.  
Об'єкт:  
процес захисту інформації.

Предмет:  
технічна система захисту  
інформації від витоку  
матеріально-речовим каналом.

1

### РОЗДІЛ 1

Проаналізовано технічні канали витоку інформації та визначено специфіку матеріально-речового каналу.

2

### РОЗДІЛ 2

Розглянуто функціональність технічних систем охорони, способи побудови та склад засобів контролю.

3

### РОЗДІЛ 3

Запропоновано технологію захисту інформації від витоку матеріально-речовим каналом.

4

### ВИСНОВКИ

Сформовано практичні рекомендації щодо підвищення ефективності захисту об'єкта інформаційної діяльності.

## ПЕРШИЙ РЕЗУЛЬТАТ

### ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ НА ОІД

матеріально-речовий

акустичний

радіоканал

електричний

оптичний

↑  
Загальна структура каналу:  
джерело сигналу → середовище  
поширення → отримувач сигналу

Інформаційний канал формується за наявності джерела, носія/середовища та засобів отримання сигналу.

Матеріально-речовий канал має особливість: витік пов'язаний із фізичним переміщенням носія інформації.

## МАТЕРІАЛЬНО-РЕЧОВИЙ КАНАЛ ВИТОКУ ІНФОРМАЦІЇ

### Основні джерела

чернетки документів, макети, фрагменти матеріалів;  
пошкоджені або списані носії даних;  
бракована продукція та її елементи;  
місця зберігання матеріальних носіїв ІзОД.

### Типові шляхи витоку

розкрадання носіїв інформації;  
витік через персонал або обслуговуючі служби;  
потрапляння відходів виробничої діяльності за межі контрольованої зони;  
недостатній облік і контроль руху матеріальних носіїв.

## ШЛЯХИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

### Екранування

зниження побічних електромагнітних випромінювань технічних засобів

### Фільтрація

локалізація небезпечних сигналів у колах живлення та з'єднувальних лініях

### Зашумлення

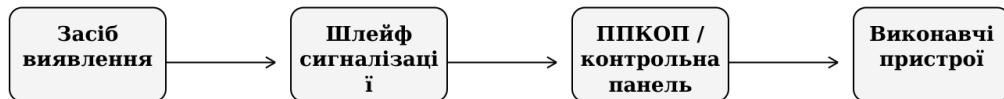
створення маскуючих перешкод для зменшення співвідношення сигнал/шум

### Технічна охорона

виявлення спроб доступу до носіїв та контроль периметрів і приміщень

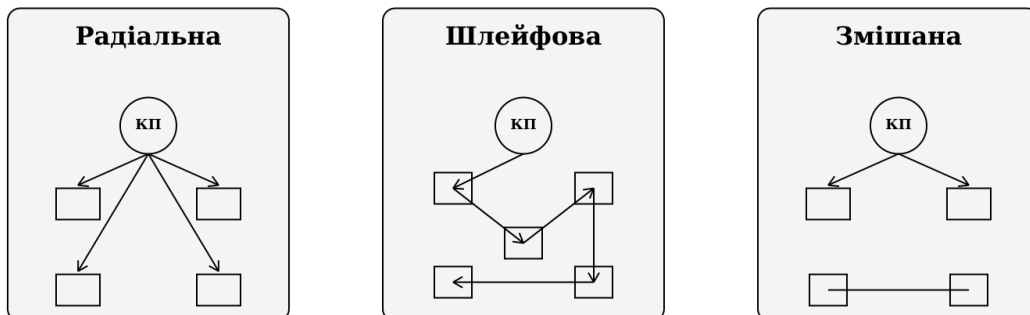
- Пасивні методи зменшують рівень небезпечного сигналу.
- Активні методи формують перешкоди та ускладнюють отримання інформативних ознак.
- Для матеріально-речового каналу ключову роль відіграє технічна система охорони та контроль матеріальних носіїв.

## ТЕХНІЧНА СИСТЕМА ОХОРОНИ ЯК ЗАСІБ ПРОТИДІЇ ВИТОКУ



- ТСО забезпечує постановку та зняття приміщень з охорони.
- Система формує сигнал тривоги при спробі несанкціонованого проникнення.
- Події можуть фіксуватись, відображатись на автоматизованому робочому місці та передаватись черговому персоналу.

## СПОСОБИ ПОБУДОВИ ТЕХНІЧНИХ СИСТЕМ ОХОРОНИ



- Вибір структури залежить від кількості засобів виявлення, ступеня централізації, особливостей об'єкта, вартості та надійності.
- Комбіновані схеми дозволяють гнучко адаптувати ТСО до складної структури об'єкта.

### КОНТРОЛЬ ПЕРИМЕТРІВ ОБ'ЄКТІВ

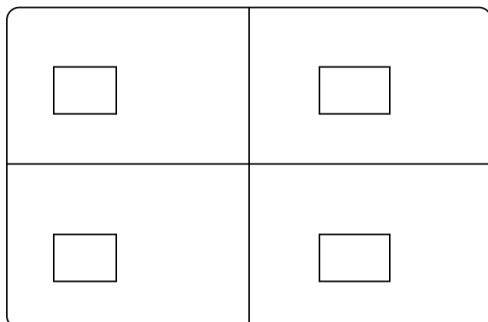
**Сейсмічні засоби** реєстрація коливань ґрунту або конструкцій

**Інфрачервоні рубежі** контроль перетину охоронної зони

**Магнітоконтактні сповіщувачі** контроль відкривання дверей, люків, воріт

**Оптичні засоби** виявлення порушення світлового променя

### ЗАСОБИ КОНТРОЛЮ ВНУТРІШНІХ РУБЕЖІВ



Умовна схема зон контролю приміщення

пасивні інфрачервоні сповіщувачі контролюють рух у приміщенні;

активні сповіщувачі формують контрольований рубіж;

комбінування датчиків підвищує достовірність виявлення;

внутрішні рубежі доповнюють периметровий захист.

### ПРИЙМАННЯ ТА ОБРОБКА СИГНАЛІВ СПОВІЩУВАЧІВ



Система повинна забезпечувати достовірне приймання тривожних сигналів і відокремлення реальних подій від завад.

Важливими є протоколювання, індикація стану зон, формування повідомлень і контроль працездатності засобів.

Централізована обробка підвищує оперативність реагування на загрози матеріально-речового витоку.

### ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ



- Технологія орієнтована на захист матеріальних носіїв та контроль переміщення предметів, які можуть містити ІзОД.
- Ефективність досягається поєднанням організаційних заходів, технічної охорони, обліку носіїв і контролю подій безпеки.

### ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ

організувати облік і маркування матеріальних носіїв інформації з обмеженим доступом;

використовувати багаторубежеву технічну систему охорони для контролю периметра, приміщень та місць зберігання;

застосовувати комбіновані сповіщувачі для зменшення імовірності пропуску порушника;

реалізувати централізоване протоколювання подій та контроль дій персоналу;

регламентувати порядок знищення чернеток, відходів і непридатних носіїв.

## ВИСНОВКИ

### ОСНОВНІ ВИСНОВКИ ЗА РЕЗУЛЬТАТАМИ РОБОТИ

- Матеріально-речовий канал витоку інформації пов'язаний із фізичним переміщенням носіїв, відходів виробництва, документів або інших предметів, що містять інформативні ознаки.
- Для протидії такому каналу доцільно використовувати комплекс організаційних, режимних і технічних заходів.
- Технічна система охорони є ключовим елементом контролю спроб винесення, викрадення або несанкціонованого доступу до матеріальних носіїв.
- Запропонована технологія захисту підвищує контрольованість об'єкта інформаційної діяльності та зменшує ризик витоку інформації матеріально-речовим каналом.

**Дякую за увагу**