МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ТЕХНОЛОГІЇ СТВОРЕННЯ ТА ЗАСТОСУВАННЯ КОМПЛЕКСІВ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ ТА ОХОРОНИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Конспект лекцій

Для студентів з галузі знань F «Інформаційні технології»
за спеціальністю F5 «Кібербезпека та захист інформації»

Київ 2026

Конспект лекцій для студентів другого (магістерського) рівня вищої освіти з дисципліни «Технології створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони об’єктів інформаційної діяльності»/ Укладачі: Туровський О.Л. д.т.н. професор, А.М. Котенко к.т.н. доцент, – К.:ДУІКТ, 2026. – 94 с.

Укладачі:
Туровський О.Л., д.т.н. професор
Котенко А.М., канд. техн. наук, доцент

Рецензент Щавінський Ю.В. - канд. техн. наук, доцент

Конспект лекцій затверджено на засіданні кафедри технічних систем кіберзахисту протокол № 17 від 04 червня 2026 р.

Схвалено Вченою радою Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій, (протокол № 12 від 09.06.2026 р).

ЗМІСТ

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

1. **Лекції** з дисципліні «Програмно-апаратні засоби захисту» у студентів спеціальності 125 «Кібербезпека та захист інформації» охоплюють розділи курсу, що пов'язані з розглядом причин втрати інформації та методами і засобами захисту інформації від втрат.

2. Мета лекційних занять полягає у ознайомленні студентів з існуючими програмно-апаратними методами та засобами захисту інформації.

3. Основною метою курсу є формування у студентів теоретичного розуміння та відповідних практичних навичок, необхідних для забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності.

Інформаційно-комунікаційні системи, що використовуються для обробки інформації та інформаційного обміну, знаходяться у спеціалізованих приміщеннях – об'єктах інформаційної діяльності (ОІД). Тому в даному конспекті лекцій розглянуто фізичні причини виникнення радіоканалу (побічні електромагнітні випромінення (ПЕВМ) технічних засобів) та електричного (наведення ПЕВМ та просочування інформаційних сигналів в електричні лінії) витоку інформації. Розглянути активні та пасивні методи та засоби протидії витоку інформації через електричний та радіоканал.

Акустичний канал витоку інформації з ОІД виникає під час озвучування секретної інформації на ОІД. В даному конспекті лекцій розглянуто фізичні причини виникнення акустичного каналу як то – за рахунок вібрації інженерних конструкцій ОІД, акустоелектричних та параметричних перетворювань тощо. Розглянуто активні та пасивні методи та засоби протидії витоку акустичної інформації з ОІД.

Розглянуто причини виникнення матеріально-речового каналу витоку інформації з ОІД, та методи і засоби протидії даній загрозі інформації.

2 ЛЕКЦІЙНИЙ МАТЕРІАЛ

Лекція № 1

Тема. Технічні канали витоку інформації

ПЛАН ЛЕКЦІЇ

1. Загрози інформації
2. Небезпечні сигнали та їх джерела
3. Класифікація технічних каналів витоку інформації

1. Загрози інформації

Впливи які створюються зловмисниками на інформацію є навмисними. До них відносяться як безпосередній вплив зловмисника на джерело інформації так і вплив полів та електричних сигналів технічними засобами, що створюється людиною, з метою знищення, зміни або крадіжки інформації.

Ці впливи створюють *канал несанкціонованого доступу до інформації*. Якщо впливи цілеспрямовано створюються то канал несанкціонованого доступу називається навмисний, якщо сили випадкові то канал НСД зветься випадковий.

Навмисний канал НСД створюється зловмисником.

Типові причини створення каналу несанкціонованого доступу:

- виконання операції по здобуванню інформації розвідкою іноземної держави;
- спроба несанкціоновано отримати інформацію співробітником організації для її продажу, шантажу;
- несправність програмно-апаратних засобів зберігання, обробки передачі інформації;
- помилки персоналу при обробці інформації.

Несанкціоноване розповсюдження інформації від її джерела до зловмисника називається *витоком інформації.*

Розрізняють:

- спостереження – прийом оптичних та інших сигналів для отримання зображень;
- прослуховування – прийом та аналіз акустичних сигналів.
- перехоплення – прийом та аналіз радіо та електричних сигналів.

Прослуховування розуміє використання різних технічних засобів. Цим способом здобувається різноманітна мовна інформація.

Спостереженням добувається видові ознаки об'єктів, але можливе добування семантичної інформації. Для добування інформації також застосовуються технічні засоби: відеокамери видимого діапазону, прилади чутливі до ІЧ випромінення, радіолокаційне спостереження.

Перехоплення розуміє несанкціонований прийом радіо та електричних сигналів і вилучення з них семантичної інформації, демаскуючих ознак сигналів, формування зображення об'єктів.

Різномаїття технічних засобів та їх комплексне застосування для отримання інформації іноді розмивають грані між розглянутими способами. Наприклад при перехоплення сигналів состового зв'язку здійснюється підслуховування розмови між абонентами, тобто одночасно здійснюється перехоплення і прослуховування. Враховуючи неоднозначність понять *Перехоплення та Прослуховування,* способи добування акустичної інформації відносять до прослуховування а несанкціонований прийом радіо та електричних сигналів до *Перехоплення.*

Шлях несанкціонованого розповсюдження інформації від джерела до зловмисника називається ***каналом витоку інформації*** [1,2,3]. Якщо розповсюдження інформації здійснюється за допомогою технічних засобів то канал витоку інформації називається ***технічним каналом витоку інформації***. Загрози витоку бувають *випадкові* та такі *навмисно* створювані зловмисником. Якщо характеристики джерел сигналів зловмиснику апріорі невідомі, то технічні канали витоку інформації називаються інформації називаються *випадкові*. Якщо технічний канал витоку інформації організується зловмисником наприклад за допомогою закладного пристрою (подслушка) то такий канал витоку інформації називається *організованим*.

Загроза витоку інформації оцінюється по величині шкоди, яка виникає при її реалізації. Розрізняють *потенційну* та *реальну* шкоду. Потенційна шкода існує при появі загрози. Реальна – при реалізації загрози витоку. Ймовірність або ризик виникнення загрози залежить від багатьох факторів. Основні з них:

- ціна інформації;
- рівень захищеності інформації;
- кваліфікація зловмиснику, його витрати на здобування інформації;
- криміногенна обстановка у місці знаходження організації.

2. Небезпечні сигнали

Носії інформації у вигляді електричного струму та полів називаються *сигналами*. Якщо інформація, що міститься в сигналах таємна, а сигнали можуть

бути прийняті зловмисникомі і з них знята ці інформація, то такі сигнали являють собою небезпеку для інформації і називаються *небезпечними*.

Небезпечні сигнали можуть бути *функціональними та випадковими*.

Функціональні сигнали створюються радіотехнічним засобом. Для виконання ним функцій по обробці, передачі, зберігання інформації. При передачі таємної інформації функціональними сигналами, її відправник розуміє потенційні загрози безпеці інформації.

Основні джерела функціональних сигналів:

передавачі систем зв'язку;

передавачі радіотехнічних систем;

випромінювачі акустичних сигналів;

Засоби систем зв'язку створюють найбільш багаточисленну групу джерел з семантичною інформацією. Сюди відносяться засоби радіозв'язку, проводний, радіорелейний, космічний зв'язок.

Також джерелами радіосигналів, що випромінюються навколо являються стаціонарні та мобільні радіопередавальні пристрої систем радіозв'язк, а електричних сигналів що передаються по проводам – телефонні, телеграфні прилади; ПЕОМ що обєднані мережею, модеми апаратури передачі даних.

Також в останній час для передачі інформації в якості джерел сигналів використовують лазери оптичних засобів зв'язку. Оптичні системи мають значно кращі показники по смузі пропускання та завадостійкості. Кабелі волоконно-оптичних систем зв'язку поступово витісняють кабелі пропводних систем електрозв'язку.

Радіо, електричні та світові сигнали циркулюють як внутрі організації так і можуть розповсюджуватись на великі відстані. Враховуючи широке застосування засобів зв'язку і велику дальність їх розповсюдження, перехоплення сигналів засобів зв'язку є дуже ефективним та розповсюдженим методом отримання інформації.сигнали засобів зв'язку містять не тілки семантичну інформацію, а й інформацію про ознаки сигналів та місце розташування самих засобів зв'язку.

До радіотехнічних систем та засобів відносяться засоби радіолокації, радіотелеметрії та радіопротидії (РЕБ).

Але потенційна небезпека для інформації, яка міститься в функціональних сигналах відома її власнику. Він може прийняти міри для зниження небезпеки.

Однак робота радіоелектронних засобів що використовуються для прийому, обробки та зберігання інформації супроводжується фізичними процесами та явищами які стіорюють прбічні радіо та електричні сигнали. Якщо ці сигнали містять секретну інформацію і к ним можливий доступ технічних засобів зловмисника, то небезпека до цієї інформації значно вища ніж для аналогічної інформації що міститьсяв функціональних сигналах. Такі сигнали, що

виникають випадково, називаються *випадковими небезпечними сигналами.* Ці сигнали виникають в силу фізичних процесів, незалежно від користувача цього засобу. Користувач без проведення спеціальних досліджень може й не знати про їх існування і що інформація піддається небезпеці. В цьому полягає відмінність функціональних небезпечних ситналів від випадкових небезпеяних сигналів. До технічних засобів обробки інформації які створюють небезпечні сигнали відносяться:

засоби телефонного проводного зв'язку;

засоби мобільного телефонного та радіозв'язку;

засоби електронної обчислювальної техніки;

радіоприйомні паристрої;

телевізійні засоби.

Крім того випадкові небезпечні сигнали створюються електричними приладами:

засоби охоронної та пожежної сигналізації;

засоби кондиціонування повітря;

побутові прилади, оргтехніка та інше обладнання яке має у своєму складі елементи перетворення акустичної інформації у електричні сигнали;

електропроводящі комунікації будівлі які проходять через контрольовану зону.

Характеристики випадкових небезпечних сигналів радіоелектронних засобів апріорі невідомі ні зловмиснику ні користувачеві. Для їх пошуку та визначення характеристик проводять спеціальні дослідження цих засобів.

Усі технічні засоби на об'єктах інформаційної діяльності діляться на основні технічні засоби та системи (ОТЗС) та допоміжні технічні засоби та системи (ДТЗС).

До ОТЗС відносяться засоби та їх комунікації які забезпечують обробку, зберігання та передачу інформації яку потрібно захищати.

Якщо технічний засіб на ОІД не призначено для обробки таємної інформації його називають ДТЗС. ДТЗС знаходяться у одному приміщенні з ОТЗС. З цього слідує, що ДТЗС необхідно розглядати як потенційні джерела небезпечних сигналів. До ДТЗС наприклад відносяться:

телефонні засоби та системи;

засоби охоронно-пожежної сигналізації

засоби кондиціонування повітря;

засоби електронної оргтехніки;

засоби проводної радіотрансляційної мережі.

3. Классифікація технічних каналів витоку інформації

При обробці інформації в автоматизованих системах на об'єктах інформаційної діяльності можливий її витік так званими технічними каналами витоку.

Фізичні процеси, які у пристроях обробки інформації на ОІД при її функціонуванні, створюють у навколишньому просторі побічні електромагнітні, акустичні та інші випромінювання, які тією чи іншою мірою пов'язані з обробкою інформації.

Подібні випромінювання можуть бути виявлені на досить значних відстанях (до сотень метрів) і, отже, використовуватися зловмисниками, які намагаються отримати доступ до секретів. Тому заходи щодо ЗІ, що циркулює в технічних засобах, спрямовані насамперед на зниження рівнів таких випромінювань.

Побічні електромагнітні випромінювання виникають внаслідок непередбаченої схемою або конструкцією технічного засобу передачі інформації з паразитних зв'язків напруги, струму, заряду або магнітного поля.

Під паразитним зв'язком розуміють зв'язок електричним або магнітним ланцюгам, що з'являється незалежно від бажання конструктора. Залежно від фізичної природи елементів паразитних електричних кіл розрізняють паразитний зв'язок через загальний повний опір, ємнісний або індуктивний паразитний зв'язок.

Під технічним каналом витоку інформації розуміється сукупність фізичних полів, що несуть таємну інформацію, конструктивних елементів, що взаємодіють з ними, та технічних засобів зловмисника для реєстрації поля та зняття інформації [1] (рис. 1.1).

Рис. 1.1 Склад технічного каналу витоку інформації

Перехоплення інформації за допомогою технічних засобів може здійснюватись лише за межами контрольованої зони – території об'єкта, на якій виключено неконтрольоване перебування осіб та транспортних засобів, які не мають постійних чи разових перепусток.

Джерелами випромінювань у технічних каналах є різноманітні технічні засоби, у яких циркулює інформація з обмеженим доступом.

Такими засобами можуть бути:

мережі електроживлення та лінії заземлення;

автоматичні мережі телефонного зв'язку;

засоби звуко- та відеозапису;

електронно-обчислювальна техніка;

електронні засоби оргтехніки.

Джерелом випромінювань у технічних каналах витоку може бути голосовий тракт людини, що викликає появу небезпечних акустичних випромінювань у приміщенні чи поза нею. Середовищем поширення акустичних випромінювань у разі є повітря, а при закритих вікнах і дверях — повітря і всілякі звукопровідні комунікації. Якщо для перехоплення інформації використовується відповідна техніка, то утворюється технічний канал витоку інформації, так званий акустичним.

В загалі, в інформаційній безпеці, прийняти наступні технічні канали витоку інформації:

радіоканали (побічні електромагнітні випромінювання технічних засобів);

акустичні (поширення звукових коливань у будь-якому звукопровідному матеріалі);

електричні (небезпечні напруги та струми в різних струмопровідних комунікаціях);

оптичні канали (електромагнітні випромінювання в інфрачервоній, видимій та ультрафіолетовій частині спектру (ВОЛЗ));

матеріально-речові канали (папір, фото, магнітні носії, відходи тощо

Утворенню технічних каналів витоку інформації сприяють певні обставини та причини технічного характеру. До них можна віднести недосконаліть елементної бази та схемних рішень, прийнятих для даної категорії технічних засобів, експлуатаційне зношування елементів виробу, а також зловмисні дії.

Основними джерелами виникнення технічних каналів витоку інформації є:

перетворювачі фізичних величин;

випромінювачі електромагнітних коливань;

паразитні зв'язки та наведення на провода та елементи електронних пристроїв.

Для кожної з цих груп, у свою чергу, можна виконати декомпозицію за принципом перетворення чи іншими параметрами. Так, за принципами перетворення акустичні перетворювачі поділяються на індуктивні, ємнісні, п'єзоелектричні.

Декомпозиція випромінювачів електромагнітних коливань виконується діапазоном частот.

Паразитні зв'язки та наведення виявляються у вигляді зворотного зв'язку (найбільш характерний позитивний зворотний зв'язок), витоку по ланцюгах живлення та заземлення.

Технічні засоби та системи можуть не тільки безпосередньо випромінювати в простір сигнали, що містять оброблювану ними інформацію, але і вловлювати за рахунок своїх мікрофонних або антенних властивостей акустичні або електромагнітні випромінювання, що існують в безпосередній близькості від них. Такі технічні засоби можуть перетворювати прийняті випромінювання на електричні сигнали і передавати їх по своїм лініям зв'язку, як правило, безконтрольним, за територією об'єкта на значні відстані, що ще більшою мірою підвищує небезпеку витоку інформації.

Непоодинокі випадки, коли технічні пристрої мають у своєму складі, крім подібних "мікрофонів" і "антен", високочастотні або імпульсні генератори. Генеровані коливання в таких пристроях можуть бути промодульовані електричними сигналами, внаслідок чого ці технічні пристрої перетворюються на радіопередавачі і становлять серйозну небезпеку, оскільки здатні випромінювати інформацію в навколишній простір.

До основних інформаційних характеристик каналу належать:

форма інформації, що передається (дискретна, безперервна) у ланках каналу;

швидкість передачі та обсяг інформації, що передається;

пропускна спроможність каналу;

ємність каналу.

Параметри каналу визначаються фізичною структурою каналу, його типом та режимом використання.

Ширина смуги пропускання (частотний спектр) каналу ΔF змінюється від 3100 Гц для телефонного, до 8 МГц для телебачення і сотень мегагерц для оптичних ліній зв'язку.

Перевищення сигналу над перешкодою в каналі (динамічний діапазон), що визначається співвідношення потужностів сигналу і перешкоди в каналі, - здатність каналу передавати різні рівні сигналу. Динамічний діапазон обмежує дальність передачі, і навіть впливає можливість виділення сигналу на фоні перешкод:

$$Д = 10\log(P_с / P_п),$$

де:

$P_с$ $P_п$ — середні потужності сигнала та перешкоди у каналі на вході приймача.

Кожен канал також характеризується кількістю інформації, яка може бути передана ним.

Максимальне значення кількості інформації, яка може бути передана каналом зв'язку, що має смугу пропускання F, визначається формулою Шеннона:

$$C_{max} = F_к \log(1 + P_с / P_ш) \text{ [дв.одиниць/с]}$$

де:

$P_с$ — середня потужність сигналу, $P_ш$ — потужність шуму з рівномірним частотним спектром.

Як у будь-якій системі зв'язку, у каналах витоку інформації небезпечний сигнал (сигнал, що несе секретну інформацію) характеризується тривалістю $T_с$, динамічним діапазоном Dc та шириною спектру $F_с$, добуток яких представляє його об’єм $V_с = T_с \cdot F_с \cdot D_с$.

У тривимірному просторі обсяг сигналу можна подати у вигляді паралелепіпеда (рис. 1.2).

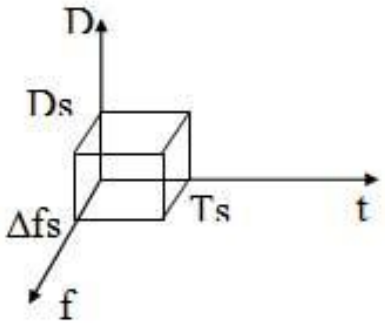

Рис. 1.2 Інтерпретація об’єму сигналу у тривимірному просторі

Якщо об’єм сигналу перевищує об’єм каналу передачі цього сигналу, то цим каналом зв'язку передача сигналу без втрати інформації неможлива. Тобто:

Vk .> Vc

Об’єм каналу визначається як:

Vk = Dk Fk Tk

де:

Tk – час впродовж якого передається сигнал.

Для забезпечення неспотвореної передачі повідомлення визначеним об’ємом необхідно, щоб характеристики середовища розповсюдження та приймача відповідали ширині спектру сигналу та його динамічному діапазону.

Якщо полоса частот середовища розповсюдження або приймача вуже полоси сигналу то для забезпечення неспотворпеної передачі сигналу об’ємом Vc необхідно зменшити ширину його спектру. При цьому для забезпечення Vc = const відповідно необхідно збільшити час передачі сигналу Tc. Для неспотвореної передачі повідомлення у реальному масштабі часу смуга пропускання приймача повинна відповідати смузі спектра сигнала.

Узагальнена модель технічного каналу витоку інформації

Основою всіх сучасних технічних засобів є електронні та радіоелектронні пристрої. Фізичні процеси, що відбуваються в цих пристроях, створюють при обробці закритої інформації об'єктивні передумови для появи небезпечних сигналів в навколишньому просторі, сторонніх інформаційних лініях, ланцюгах електроживлення, заземлення і т. д., що створює реальні умови для отримання передбачуваним противником закритих відомостей, що циркулюють технічні засоби, за допомогою засобів розвідки.

Фізичні явища, що лежать в основі появи небезпечних сигналів за межами контрольованої зони, та шляхи їх можливого витоку можуть бути різними. Тим не менш, у загальному вигляді витік інформації може розглядатися як ненавмисна передача закритої інформації деякою побічною системою зв'язку.

Перехоплення інформації за допомогою технічних засобів розвідки може здійснюватися лише за межами контрольованої зони – території об'єкта, де виключено неконтрольоване перебування осіб і транспортних засобів, які мають постійних чи разових перепусток.

В даний час перехоплення може бути організовано:

з території посольства, місій, представництв іноземних держав та з належних їм будівель;

із місць постійного чи тимчасового проживання іноземних громадян (житлових будинків, дач, готелів);

із місць постійного чи тимчасового проживання розвідників;

із дипломатичних автомобілів, обладнаних спеціальною технікою;

з вулиць та транспортних засобів при розміщенні спец. апаратури в одязі, сумці, валізі тощо;

із схованок, розміщених поблизу об'єкта захисту, із застосуванням закамуфльованих автономних пристроїв технічної розвідки.

Контрольні запитання

1. Які існують групи загроз по виду реалізації
2. Причини виникнення каналів несанкціонованого доступу до інформації
3. Що називається витоком інформації і які причини її виникнення
4. Що називається технічним каналом витоку інформації
5. Чим оцінюється загроза витоку інформації
6. Що є джерелом загроз випадкових впливів
7. Які сигнали називаються небезпечними
8. Що відноситься до основних і допоміжних технічних засобів і систем при обробці інформації
9. Що розуміється під технічним каналом витоку інформації
10. Які існують технічні канали витоку інформації
11. Яка умова неспотвореної передачі сигналу по каналу зв'язку
12. Що називається об'ємом сигналу
13. Що вілноситься до основних інформаційних характеристик каналу зв'язку.

Лекція № 2

Тема. Несанкціоноване отримання акустичної інформації

ПЛАН ЛЕКЦІЇ

1. Засоби несанкціонованого отримання акустичної інформації
2. Пристрої прослуховування приміщень

1. Засоби несанкціонованого отримання акустичної інформації

Найбільш поширеними засобами несанкціонованого отримання інформації, з якими фахівцям із захисту інформації часто доводиться стикатися на практиці [2, 3]:

1. Радіозакладки - мікропередавачі, радіус дії яких, як правило, не перевищує кількох сотень метрів. Сучасна елементна база дозволяє створювати радіозакладки в домашніх умовах.

2. Спрямовані мікрофони, що мають голчасту діаграму спрямованості. За допомогою такого мікрофона можна прослухати розмову на відстані до 1 км у межах прямої видимості. За автомобілем, що рухається, аудіоконтроль вести можна тільки в тому випадку, якщо в ньому заздалегідь була встановлена закладка. На тривалих зупинках розмову можна прослуховувати спрямованим мікрофоном за умови, що автомобіль знаходиться в зоні прямої видимості і в ньому опущено одне зі стекол. У громадських місцях (кафе, ресторани тощо) прослуховування можна здійснювати спрямованим мікрофоном або закладкою. У таких випадках гучна музика, як втім і шум води, що ллється, не рятують, так як у спрямованого мікрофона дуже вузька діаграма спрямованості.

3. Засоби прослуховування телефонних розмов можуть здійснювати несанкціоноване отримання інформації за телефонною лінією кількома методами:

- встановлення записуючої апаратури записуючої апаратури на АТС з використанням недобросовісності чи недбалості обслуговуючого персоналу;
- безпосереднє підключення записуючої апаратури до телефонної лінії (наприклад, у розподільчій коробці);
- вбудовування схеми несанкціонованого підключення до телефону (для цього необхідний доступ до приміщення, в якому встановлено цей апарат).

4. Якщо у приміщенні шибки не завішені, то розмову за такими вікнами можна прослухати, направивши на скло лазерний промінь. Звукові коливання в приміщенні призводять до синхронної вібрації скла, а вони модулюють лазерний промінь, що відбивається від скла і приймається приймальним пристроєм.

5. У приміщеннях, в яких не було проведено спеціальних заходів щодо ЗІ, можна прослуховувати за допомогою пристроїв, що реєструють коливання елементів конструкції будівлі (розетки, батареї центрального опалення, вентиляція, тонкі перегородки тощо).

2. Пристрої прослуховування приміщень

До цієї групи пристроїв відносяться: приймальна апаратура, мікрофони, електронні стетоскопи, магнітофони та апаратура прослуховування телефонів.

Прослуховування - спосіб ведення розвідки, що застосовується агентами, спостерігачами, спеціальними постами прослуховування. Це один із поширених способів отримання (добування) інформації.

Прослуховування може здійснюватися безпосереднім сприйняттям акустичних коливань при прямому сприйнятті мовної інформації, або сприйнятті звукових коливань, що надходять через елементи будівель та приміщень (стіни, підлоги, стелі, вентиляційні канали, системи опалення), а також за допомогою різноманітних технічних засобів. До цього слід додати, що прослуховування ведеться в реальному масштабі часу та певною мірою може дозволити своєчасно ухвалити важливі оперативні рішення.

Прослуховування можна класифікувати так:

1. Безпосереднє

- пряме;
- через конструкції будівель та приміщень.

2. За допомогою технічних засобів

- за допомогою мікрофонів;
- за допомогою радіозакладок;
- лазерне підслуховування;
- метод високочастотного нав'язування.

Пристрої аудіоспостереження, за допомогою яких ведеться прослуховування, легко встановити і вкрай важко виявити, оскільки сучасна апаратура є мініатюрною, надійною і має тривалий термін дії.

Широке поширення набули системи з акустоавтоматикою, що включаються автоматично під час звуку голосу.

Спрямований мікрофон.

Використання явища резонансу звукових хвиль у спрямованих системах призводить до збільшення звукової енергії, що надходить мікрофон. Найпростіший спрямований мікрофон фізично являє собою вибіркову резонансну система, а конструкційно набір з 10 і більше алюмінієвих трубок діаметром 10 мм Довжина трубки визначає її резонансну частоту. Довжині трубки 20 мм відповідає

частота 8200 Гц, довжині 92 мм - частота 180 Гц и т.д. Довжину трубки можна розрахувати за виразом:

$$L_{(м)} = 330/2F,$$

де:

F - частота звуку (Гц)

Мікрофон встановлюється в параболічному уловлювачі, фокусом якого є спрямовуюча система виконана з трубок. Для подальшого посилення використовується високочутливий малошумний мікрофонний підсилювач. Для прослуховування розмови можна обмежитися набором з 7 трубок, оскільки основний частотний діапазон людської мови лежить у межах 180-2150 Гц. Використовується в основному для прослуховування за межами приміщень.

Сучасні спрямовані мікрофони класифікуються наступним чином:

- параболічні мікрофони. Вони збирають звукові хвилі у фокус параболи. Високоефективні, проте габаритні;
- мікрофони-гармати. Конструктивно являють собою трубку-хвилевод в якій встановлено мікрофон.

На рис. 2.1 приведено вигляд сучасного спрямованого мікрофона-гармати KMR-359 з пристроєм обробки акустичної інформації [4]. Такий мікрофон ефективний на відкритій місцевості на дальності до 150 м У міській смузі його параметри скромніші, дальність прослуховування - 20 - 50 м

Якщо немає можливості встановити пристрій стеження безпосередньо в приміщенні, інформація може бути отримана за допомогою акустичних стетоскопів, які дозволяють прослуховувати розмови через вібрацію інженерних конструкцій ОІД як то дверей, стель, вікон та бетонні стіни товщиною 50 - 70 см або вікна, що прилягають до контрольованого приміщення (рис. 2.2) [5].

Рис. 2.1 Професійний спрямований мікрофон KMR-359

Рис. 2.2 Сучасний акустичний стетоскоп

Часто для перехоплення розмов використовуються мініатюрні магнітофони. Такі пристрої вловлюють мову з відстані 8 - 10 м і здебільшого мають інтегрований акустоматик. Форма та розміри таких пристроїв дозволяють їх легко приховати, наприклад, у книзі середнього об'єму.

Найбільш дорогими пристроями, що перехоплюють акустичні сигнали є оптико-електронні (лазерні системи). На вікно спрямовується невидимий лазерний промінь, який модулюється коливаннями скла і відбивається на оптичний приймач, що перетворює його на аудіо сигнали. На (рис. 2.3) [6] представлено зовнішній вигляд та будова сучасного оптико-електронного (лазерного стетоскопа).

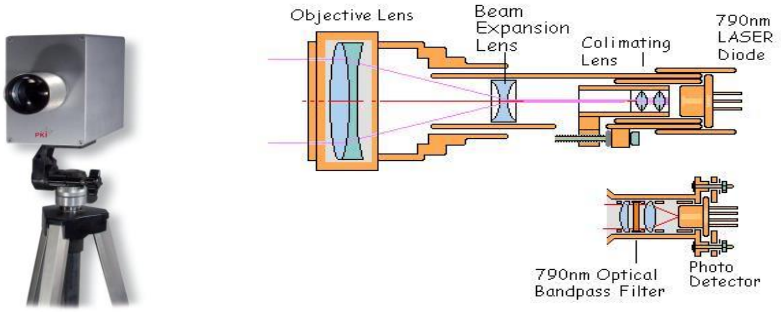

Рис. 2.3 Сучасний оптико-електронний (лазерний стетоскоп)

Важливим джерелом отримання інформації є лінія зв'язку, зокрема телефон. Прилади телефонного прослуховування можуть підключатися до будь-якої точки лінії, часто замасковані під різні деталі апарата. Закладки мають необмежений термін служби, оскільки живляться від телефонної лінії, причому функціонування телефону та лінії не порушується. Особливий інтерес становлять передавачі телефонного та кімнатного прослуховування, які після закінчення

телефонної розмови автоматично перемикаються на спостереження за контрольованим приміщенням.

Поєднання відносно невисокої ціни і виключно високої ефективності таких пристроїв, а також відсутність суворих правових норм роблять цей шлях витоку інформації одним із найнебезпечніших.

До основних типів закладних пристроїв прослуховування, що використовують радіоканал, відносяться:

- закладні пристрої (радіомікрофони);
- телефонні закладки (або комбіновані варіанти із радіомікрофонами).

Закладки представлені широким спектром різноманітних варіантів виконання. Встановлення радіозакладок у технічні засоби забезпечення виробничої діяльності виконується з метою одержання конфіденційної інформації акустичного характеру або інформації, що передається (опрацьовується) такими технічними засобами в електронній або електромагнітній формі.

Сигнал приймається звичайними або спеціальними радіоприймачами і фіксується на відповідній кінцевій апаратурі. Радіозакладки забезпечують реалізацію одного з найпоширеніших способів несанкціонованого доступу до джерел інформації - прослуховування. При цьому розмови, що перехоплюються, або звукові сигнали техніки та обладнання надходять до зловмисника на радіочастотах по радіо або провідному каналам.

Мікрофонні радіозакладки - це мініатюрні радіопередавачі з вбудованим або винесеним мікрофоном. Останні застосовуються, якщо радіопередавач за будь-якими умовами не може передавати інформацію з певної зони, наприклад, через особливості поширення радіохвиль або жорсткого режиму радіоконтролю. Масштабність застосування радіозакладних пристроїв пояснюється ще й тим, що їх виготовлення доступне не тільки спеціалізованим організаціям, а й радіоінженеру початківцю.

Сучасні радіозакладні пристрої для передачі акустичної інформації використовують також сучасні технологічні цифрові комунікаційні рішення як то GSM мережу рис. 2.4 [7].

Рис. 2.4 GSM радіозакладний пристрій

За допомогою звичайного мобільного телефона можливо прослуховувати розмови які ведуться у радіусі дії GSM-передавача. Об’єкт спостереження може знаходитись від приймача звуку доволі далеко. Для того щоб почати прослуховування необхідно просто зателефонувати на встановлену у закладку SIM-карту. Живлення пристрою здійснюється від акумуляторної батареї. Спектр використання такого рішення дуже широкий.

Також у якості каналу передачі аудіо інформації закладні пристрої використовують Wi - Fi мережу рис. 2.5 [8].

Рис. 2.5 Радіозакладний пристрій з використанням Wi-Fi мережі

Такий закладний пристрій непомітно встановлюється в приміщенні та підключається до місцевої Wi-Fi мережі. Він записує звук (можливо активується лише на голос для економії заряду) і транслює аудіопотік у реальному часі через спеціальний мобільний додаток або завантажує файли у хмару. На відміну від класичних GSM - закладок, які потребують SIM-карти та створюють витрати на мобільний зв'язок, Wi-Fi пристрої використовують безкоштовне інтернет-підключення.

Закладні пристрої можуть використовувати для передачі аудіоінформації ще одну із сучасних цифрових комунікацій – технологію DECT. При використанні DECT закладка реєструється у легальній DECT - мережі як звичайна бездротова трубка і після цього може передавати аудіосигнал на сторонню базову станцію. Живиться така закладка від автономного джерела електроживлення. Такі пристрої працюють на частоті 1880 – 1900 МГц. Реалізується дана технологія одним з двох наступниз шляхів:

1. Шляхом модифікації DECT – телефонів. Зі стандартного бездротового телефону виймається радіопередавач. Його під’єднують до мікрофона або напряму до телефонної лінії (для активації при виклику).

2. Спеціалізовані саморобні закладки. Створюються на базі DECT - модулів (наприклад, від старих радіотрубок), які програмуються на автоматичний підйом трубки при надходженні виклику із заданого номера.

Процес пошуку закладних пристроїв, що використовують сучасні цифрові комунікації, є складним, вимагає використання спеціального обладнання [9].

Виявити радіозакладку, що використовує аналоговий радіосигнал для передачі інформації не предствляється складним. Для цього потрібен скануючий приймач, детектор електромагнітного поля і тестове джерело звуку.

Телефонні радіозакладки можуть встановлюватися у телефонні апарати або телефонну лінію в будь-якій точці між телефоном і АТС. Вони призначаються для прослуховування розмов з передачею їх зловмиснику на радіочастотах по ефіру. Телефонні радіозакладки також є мініатюрним радіопередавачем, як мікрофон якого використовується мікрофон телефонної трубки. Зручність такого рішення полягає в тому, що джерелом електроживлення закладки є телефонна лінія, що забезпечує її роботу до тих пір, поки працює АТС. Перевагою телефонної радіозакладки є те, що прослуховується розмова обох абонентів, де б вони не розташовувалися. Під'єднуватися телефонна радіозакладка може не тільки в телефонний апарат, а й у телефонну лінію і встановлюватися навіть поза приміщенням, де розташований телефон: у телефонній розетці, у коридорі на комутаційній коробці, у розподільчій шафі і навіть на самій АТС.

За конструктивними особливостями і принципом дії радіовипромінюючі пристрої, що прослуховують, можна *класифікувати* наступним чином.

За живленням:

- з автономним живленням;
- із зовнішнім живленням (від мережі змінного струму, від телефонної лінії тощо).

За тривалістю роботи:

- необмежено (живлення від зовнішнього джерела);
- від кількох годин до кількох тижнів.

По дальності дії: від одиниць до сотень метрів.

За конструктивним виконанням:

- з камуфляжем під різні електро та побутові предмети;
- без елементів камуфляжу.

По частотному діапазону: від десятків кГц до сотень, а окремих випадках і тисяч МГц (найчастіше використовуються такі діапазони: 60-170, 250-290, 310-335, 360-430 і 470-1300 МГц).

За часом включення (роботи):

- на запит;
- безперервно.

Малі габаритні розміри, маса та використання елементів камуфляжу визначають широкий діапазон варіантів використання пристроїв, що прослуховують, і ускладнює їх виявлення. Радіозакладки підбираються індивідуально для конкретного приміщення. Це необхідно для того, щоб максимально ефективно використати можливості закладки.

Контрольні запитання

1. Назвати найпоширеніші засоби несанкціонованого отримання акустичної інформації, з якими спеціалістам часто доводиться стикатися на практиці?
2. Пояснити принцип дії електронного стетоскопу.
3. Пояснити для чого використовується лазерний стетоскоп?
4. Пояснити принцип дії мікрофонної радіозакладки?
5. Розповісти про телефонну радіозакладку?
6. Як класифікуються радіозакладні пристрої по: живленню, тривалості роботи, виду модуляції сигналу?
7. Для чого використовується спрямований мікрофон. Його принцип дії.
8. Розповісти про GSM закладний пристрій.
8. Розповісти про Wi-Fi закладний пристрій.
8. Розповісти про DECT закладний пристрій.
9. Що відноситься до “заходових методів”?
10. Що відноситься до “беззаходових методів”?
11. Якими приладами можливо виявити аналогову радіозакладку?

Лекція № 3

Тема. Загрози інформації в автоматизованих системах. Радіоелектронний канал витоку інформації

ПЛАН ЛЕКЦІЇ

1. Класифікація загроз інформації в автоматизованих системах
2. Види і природа шляхів витоку інформації при експлуатації АС
3. Методи забезпечення захисту інформації від витоку через побічні електромагнітні випромінення
4. Оцінка рівня побічні електромагнітні випромінення

1. Класифікація загроз інформації в автоматизованих системах

Модель загроз інформації - це опис методів і засобів здійснення загроз для інформації в конкретних умовах функціонування автоматизованої інформаційної системи і можливого збитку від реалізації погрози.

Формування моделі загроз інформації є одним з головних чинників забезпечення її безпеки, оскільки безпосередньо пов'язане з вибором необхідного переліку послуг безпеки, заходів і засобів захисту, що реалізуються в автоматизованій системі (АС). Довершеність і повнота аналізу загроз дає необхідну впевненість, що враховані всі суттєві загрози безпеки інформації.

Конструктивним шляхом створення моделі загроз є формування окремих моделей загроз для кожної компоненти системи зокрема, для АС - центральний вузол АС (наприклад, центральний сервер при клієнт-серверній архітектурі тощо; окремі досить незалежні підсистеми АС; канали зв'язку і комутаційний центр окремих підсистем; вузол зв'язку з Internet і ін.) і типових об'єктів захисту (робочих станцій, серверів, мережевого обладнання ЛВС тощо). Формування окремих моделей загроз повинно здійснюватися на підставі загальної класифікації загроз інформації.

Протягом життєвого циклу кожної АС модель загроз необхідно переглядати в зв'язку з модернізацією і розвитком АС, а також періодично, в зв'язку з удосконаленням технічних і програмних засобів подолання механізмів захисту.

Згідно з нормативними документами ТЗІ (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99) за результатами впливу на інформацію і систему її обробки загрози поділяються на чотири класи:

- порушення конфіденційності інформації (отримання інформації користувачами або процесами всупереч встановленим правилам доступу);

- порушення цілісності інформації (повне або часткове знищення, викривлення, модифікація, нав'язування неправдивої інформації);

- порушення доступності інформації (втрата часткова або повна працездатності системи, блокування доступу до інформації);

- втрата спостереженості або керованості системи обробки (порушення процедур ідентифікації та аутентифікації користувачів і процесів, надання їм повноважень, здійснення контролю за їх діяльністю, відмова від отримання або пересилання повідомлень).

Для забезпечення конфіденційності, цілісності та доступності інформації, а також керованості системою (спостереженість) необхідно захищати інформацію не тільки від витоку технічними каналами та несанкціонованого доступу, а й виключати можливість негативного впливу на інформацію, втручання в процес її обробки, порушення працездатності системи. Таким чином, захищати необхідно всі компоненти АС: апаратуру та обладнання, програми, дані, персонал.

Процес прояви можливих загроз інформації (далі - загроз) і впливу їх на інформацію ґрунтується на системній класифікації (рис. 3.1):

Об'єктивні загрози викликаються стихійними природними явищами та об'єктивними фізичними процесами.

Суб'єктивні загрози є наслідком діяльності людини, технічних засобів і систем;

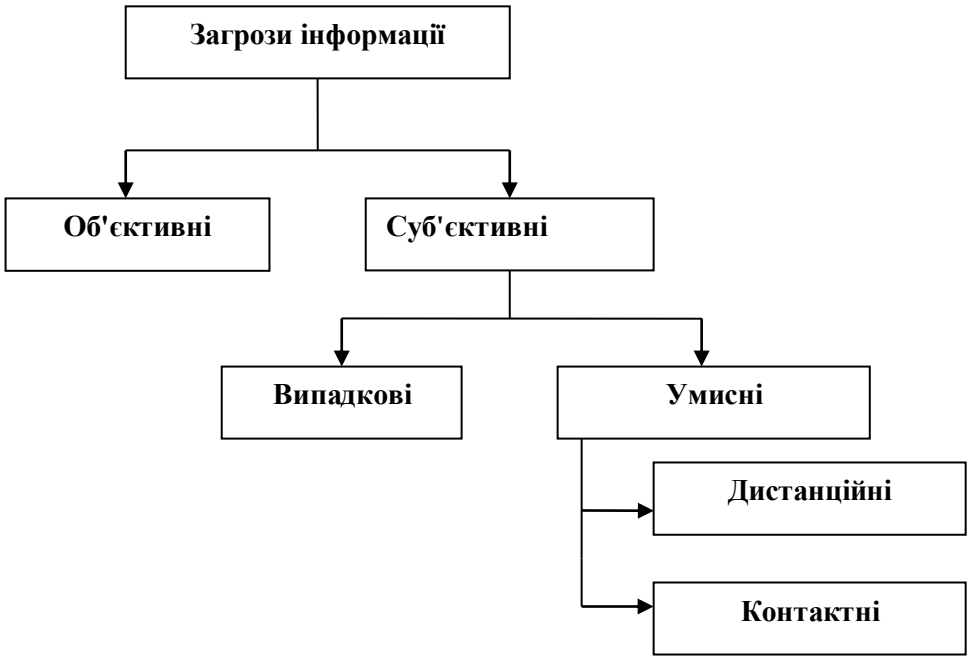

Рис. 3.1 Загальна класифікація загроз інформації в АС

- за мотивами походження суб’єктивні загрози поділяються на випадкові і навмисні. Випадкові загрози викликаються помилками проектування автоматизованої системи та системи захисту інформації, помилками в програмному забезпеченні, збоями та відмовами апаратури і систем забезпечення, помилками персоналу тощо. Навмисні загрози обумовлені цілеспрямованими діями людей (порушників);

- за місцем розміщення джерела загроз щодо автоматизованої системи навмисні загрози поділяються дистанційні та контактні. До дистанційним відносяться загрози, джерело яких знаходиться за межами контрольованої території. Контактні загрози здійснюються в межах контрольованої зони, як правило, при проникненні в приміщення, де розташовані засоби обробки і зберігання інформації.

2. Види і природа шляхів витоку інформації при експлуатації АС

З точки зору захисту інформації ці технічні пристрої є прекрасним прикладом для вивчення практично всіх каналів витоку інформації - починаючи від радіоканалу і закінчуючи матеріально-речовим [3]. Розглянемо детальніше принципи утворення каналів витоку інформації при експлуатації комп’ютера.

Як відомо, сучасні комп’ютери можуть працювати як незалежно один від одного, так і взаємодіючи з іншими комп’ютерами по комп'ютерним мережам, причому останні можуть бути не тільки локальними, а й глобальними.

З урахуванням цього фактора, повний перелік тих ділянок, в яких можуть знаходитися підлягають захисту дані, може мати наступний вигляд:

- безпосередньо в оперативній або постійної пам'яті комп’ютера;
- на знімних магнітних, магнітооптичних, лазерних та інших носіях;
- на зовнішніх пристроях зберігання інформації колективного доступу (RAID-масиви, файлові сервери і т.п.);
- на екранах пристроїв відображення (дисплеї, монітори);
- в пам'яті пристроїв введення / виведення (принтери, сканери);
- в пам'яті керуючих пристроїв і лініях зв'язку, що утворюють канали сполучення комп'ютерних мереж.

Фізично канали витоку інформації утворюються при роботі комп’ютера.

Джерелами таких каналів є:

- **електромагнітні поля (*радіоканал витоку інформації*)** - ПЕМВ (побічні електромагнітні випромінювання комп’ютера);
- **наведення струмів і напруг** у провідних комунікаціях (живлення, заземлення та з'єднувальних) ***(електричний канал витоку*)**.

Крім того, класифікацію можливих каналів витоку інформації у першому наближенні можна провести на підставі принципів, відповідно до яких

обробляється інформація, що отримується з можливого каналу витоку. Передбачаються три типи обробки: людиною, апаратурою, програмою. Відповідно до кожного типу обробки всілякі канали витоку також розбиваються на три групи. Стосовно до комп'ютера групу каналів, в яких основним видом обробки є обробка людиною, існують наступні можливі канали витоку:

- розкрадання матеріальних носіїв інформації (магнітних дисків, стрічок, карт);
- читання інформації з екрану сторонньою особою;
- читання інформації з залишених без нагляду паперових роздруківок.

У групі каналів, в яких основним видом обробки є обробка апаратурою, можна виділити наступні можливі канали витоку:

- підключення до комп'ютера спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;
- використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань комп'ютера.

У групі каналів, в яких основним видом обробки є програмна обробка, можна виділити наступні можливі шляхи втрати інформації:

- несанкціонований доступ програми до інформації;
- розшифровка програмою зашифрованої інформації;
- блокування або відключення програмних засобів захисту.

При перехоплення інформації з комп'ютера через ПЕМВ технічному контролю підлягають наступні потенційні шляхи:

- побічні електромагнітні випромінювання в діапазоні частот від 1 МГц до 1000 МГц;
- наведення ПЕМВ в мережах електроживлення, заземлення і в лініях зв'язку.

Дуже небезпечним шляхом витоку інформації є дисплей, так як з точки зору захисту інформації він є найслабшою ланкою в системі. Це обумовлено принципами роботи відеоадаптера, що складається зі спеціалізованих схем для генерування електричних сигналів управління обладнанням, яке забезпечує генерацію зображення.

Не всі ПЕМВ є небезпечними з точки зору реальної витоку інформації. Як правило, найбільший рівень відповідає неінформативним випромінюванням (в комп'ютері найбільший рівень мають випромінювання, що створюються системою синхронізації).

3. Методи забезпечення захисту інформації від витоку через ПЕМВ

Основними напрямками захисту інформації від витоку технічними каналами є:

- запобігання витоку оброблюваної інформації за рахунок побічних електромагнітних випромінювань і наведень, створюваних функціонуючими технічними засобами, а також за рахунок електроакустичних перетворень;

- виявлення впроваджених на об'єкти і в технічні засоби електронних пристроїв перехоплення інформації (закладних пристроїв).

Захист інформації, що обробляється технічними засобами, здійснюється із застосуванням пасивних і активних методів і засобів.

Пасивні методи захисту інформації спрямовані на:

- ослаблення побічних електромагнітних випромінювань (інформаційних сигналів) основних технічних засобів і систем (ОТЗС) на межі контрольованої зони до величин, що забезпечують неможливість їхнього виділення засобом розвідки на фоні природних шумів;

- ослаблення наведень побічних електромагнітних випромінювань (інформаційних сигналів) ОТЗС в сторонніх провідниках і сполучних лініях допоміжних технічних засобів і систем (ДТЗС), що виходять за межі контрольованої зони, до величин, що забезпечують неможливість їхнього виділення засобом розвідки на фоні природних шумів;

- виключення (ослаблення) просочування інформаційних сигналів ОТЗС у кола електроживлення, що виходять за межі контрольованої зони, до величин, що забезпечують неможливість їхнього виділення засобом розвідки на фоні природних шумів.

Активні методи захисту інформації спрямовані на:

- створення маскувальних просторових електромагнітних завад з метою зменшення відносини сигнал/шум на межі контрольованої зони до величин, що забезпечують неможливість виділення засобом розвідки інформаційного сигналу ОТЗС;

- створення маскувальних електромагнітних перешкод в проводах і сполучних лініях ДТЗС з метою зменшення відносини сигнал/шум на межі контрольованої зони до величин, що забезпечують неможливість виділення засобом розвідки інформаційного сигналу ОТЗС.

Класифікація способів і методів захисту інформації, що обробляється засобами цифрової електронної техніки, від витоку через ПЕМВ приведена на (рис. 3.2).

Електромагнітне екранування приміщень в широкому діапазоні частот є складним технічним завданням, вимагає значних капітальних витрат, постійного контролю і не завжди можливо по естетичним і ергономічним міркуванням. Доопрацювання засобів електронної техніки з метою зменшення рівня ПЕМВ здійснюється організаціями, що мають відповідні ліцензії. Використовуючи різні

радіопоглинаючі матеріали і схемо технічні рішення, за рахунок доопрацювання вдається істотно знизити рівень випромінювань.

Шифрування здійснюється або програмно, або апаратно за допомогою вбудованих засобів.

Активне радіотехнічне маскування передбачає формування і випромінювання маскуючого сигналу у безпосередній близькості від об'єкту, що захищається. Розрізняють декілька методів активного радіотехнічного маскування: енергетичні методи; метод "синфазної перешкоди"; статистичний метод.

При **енергетичному маскуванні методом "білого шуму"** випромінюється широкосмуговий шумовий сигнал з постійним енергетичним спектром, рівень якого істотно перевищує максимальний рівень випромінювання електронної техніки. На даний час дуже поширений. До його недоліків слід віднести створення неприпустимих перешкод радіотехнічним і електронним засобам.

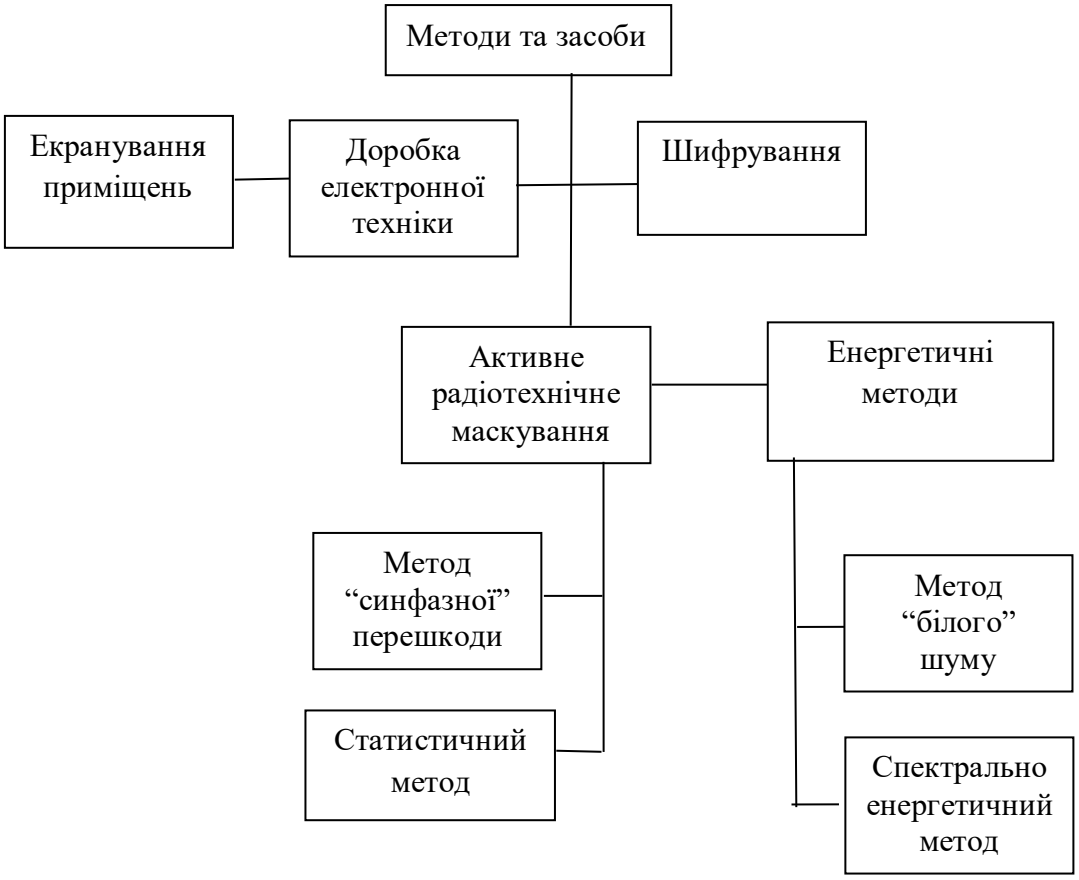

Рис. 3.2 Методи та засоби захисту інформації, що обробляється засобами електронної техніки від витоку через ПЕМВ

Спектрально-енергетичний метод полягає в генеруванні перешкоди, що має енергетичний спектр, який визначається модулем спектральної щільності інформативних випромінювань техніки. Даний метод дозволяє визначити

оптимальну перешкоду з обмеженою потужністю для досягнення необхідного співвідношення сигнал/перешкода на кордоні контрольованої зони.

Перераховані методи можуть бути використані для захисту інформації як в аналоговій, так і в цифровій апаратурі. Як показник захищеності в цих методах використовується співвідношення сигнал/перешкода.

У методі "синфазної перешкоди" в якості маскуючого сигналу використовуються імпульси випадкової амплітуди, що збігаються за формою і часу існування з корисним сигналом. В цьому випадку перешкода майже повністю маскує сигнал, прийом сигналу втрачає сенс, тому що апостеріорні ймовірності наявності і відсутності сигналу залишаються рівними їх апріорним значенням. Показником захищеності в даному методі є гранична повна ймовірність помилки (ГПВП) на кордоні мінімально допустимої зони безпеки.

Статистичний метод захисту інформації полягає в зміні ймовірнісної структури сигналу, що приймається розвідприймачем шляхом випромінювання спеціальним чином сформованого маскуючого сигналу.

До переваг даного методу варто віднести те, що рівень маскуючого сигналу не перевищує рівня інформативних ПЕМВ техніки.

Механізм виникнення ПЕМВ засобів цифрового електронного техніки.

Побічні електромагнітні випромінювання, які генеруються електромагнітними пристроями, обумовлені протіканням диференціальних і синфазних струмів.

У напівпровідникових пристроях електромагнітне поле утворюється при синхронному протікання диференційних струмів в контурах двох типів. Один тип контуру формується провідниками плати або шинами, по яких напівпровідникові прилади підключені до джерела живлення. Інший тип контура утворюється при передачі логічних сигналів від одного пристрою до іншого з використанням у якості зворотнього проводу шини живлення. Провідники передачі даних спільно з шинами живлення формують динамічно працюючі контури, що з'єднують передавальні та прийомні пристрої.

Випромінювання, викликане синфазними струмами, обумовлено виникненням падінь напруги в пристрої, що створює синфазну напругу відносно землі. Як правило, в цифровому електронному обладнанні здійснюється синхронна робота логічних пристроїв. В результаті при перемиканні кожного логічного пристрою відбувається концентрація енергії в імпульсні складові, що збігаються за часом. При їх накладенні між собою, сумарні рівні випромінювання можуть виявитися вище, ніж може створити будь-який з окремих пристроїв.

У багатьох випадках основними джерелами випромінювань виявляються кабелі, по яких передається інформація в цифровому вигляді. Такі кабелі можуть розміщуватися всередині пристрою або з'єднувати їх між собою.

Застосування у якості заземлення обплетення кабелю або проводу, які характеризуються великими індуктивністю і активним опором для ВЧ перешкод, призводить до того, що кабель починає діяти як передавальна антена.

Технічна реалізація пристроїв активного радіотехнічного маскування.

Для здійснення активного радіотехнічного маскування ПЕМВ використовуються пристрої, що створюють шумове електромагнітне поле у діапазоні частот від декількох кілогерць до 1000 МГц із спектральним рівнем, що істотно перевищує рівні природних шумів та інформаційних випромінювань ОТЗС [2, 3]. Для цих цілей використовуються малогабаритні широкосмугові передавачі шумових маскуючих коливань, наприклад генератор типу IZ 2000 (рис. 3.3) [10]. Це сучасна вітчизняна розробка від компанії “Інфозахист”.

Рис. 3.3 Сучасний генератор електромагнітного шуму IZ-2000

Сформований генератором шумовий сигнал за допомогою антени випромінюється у навколишній простір. Спектральна щільність випромінюваного електромагнітного поля рівномірно розподілена по частотному діапазону і забезпечує необхідну перевищення маскуючого сигналу над інформативним в задану кількість разів (як вимагають нормативні документи) на кордонах контрольованої зони об'єктів.

4. Оцінка рівня ПЕМВ

Оцінка рівня ПЕМВ засобів цифрової електронної техніки може проводитися з точки зору відповідності цих рівнів наступним нормам і вимогам [2, 3]:

- санітарно-гігієнічні норми;
- норми електромагнітної сумісності (ЕМС);
- норми і вимоги по захисту інформації від витоку через ПЕМВ.

Залежно від того, відповідність яким нормам потрібно встановити, використовуються ті чи інші прилади, методи та методики проведення вимірювань.

Слід зауважити, що норми на рівні ПЕМВ з точки зору ЕМС істотно (на кілька порядків) суворіше санітарно-гігієнічних норм. Очевидно, що норми, методики та прилади, які використовуються в системі забезпечення безпеки життєдіяльності, не можуть бути використані при вирішенні задач захисту інформації.

Рівні напруженості поля випромінюваних перешкод нормуються на відстані 10 або 30 м від джерела перешкод в залежності від того, де буде експлуатуватися обладнання (в житлових приміщеннях або в умовах промислових підприємств).

Наведені допустимі рівні випромінювання достатні для перехоплення ПЕМВ на значній відстані. Крім того, в діапазоні частот 0,15 -30 МГц нормуються тільки рівні напруги перешкод на мережевому устаткуванні і не нормується напруженість поля радіозавад. Дані норми при серійному випуску виконуються з якоюсь ймовірністю. Таким чином, відповідність ПЕМВ засобів цифрової електронної техніки нормам на ЕМС не може бути гарантією збереження конфіденційності інформації, що обробляється за допомогою цих засобів.

Характеристика використовуваної вимірювальної апаратури:

- діапазон робочих частот - 9 МГц - 1000 МГц;
- можливість зміни смуги пропускання;
- наявність детекторів квазіпікового, пікового, середнього і середньоквадратичного значень;
- можливість слухового контролю сигналу, що має амплітудну і частотну модуляцію;
- наявність виходу проміжної частоти і виходу на осцилограф;
- наявність комплекту стандартних калібрувальних антен.

Сучасні вимірювальні приймачі (FSC-P1, FPL1003-P2, ESVP, SMV-41) автоматизовані і оснащені відповідними інтерфейсами, що представляє можливість управляти режимами роботи приймача за допомогою комп’ютера та передавати виміряні значення на комп’ютер для їх обробки.

Крім того для вимірювання побічних ЕМВ засобів цифрового електронного техніки можуть бути використані аналізатори спектра в комплекті з вимірювальними антенами.

В процесі обробки можуть виконуватися такі функції: пошук екстремальних значень сигналу; відбір сигналів, рівень яких перевищує заданий зсув по осі частот для оптимальної реєстрації сигналу. Вбудований мікропроцесор

забезпечує обробку амплітудно-частотних спектрів, а також оптимізацію часу вимірювання і роздільної здатності для розглянутого інтервалу частот.

На відміну від завдань ЕМС, де потрібно визначити максимальний рівень випромінювання в заданому діапазоні частот, при вирішенні задач захисту інформації потрібно визначити рівень випромінювання в широкому діапазоні частот, відповідному інформативному сигналу. Тому оцінка рівня випромінювань при вирішенні задач захисту інформації повинна починатися з аналізу технічної документації та відбору електричних ланцюгів, за якими можна передавати інформацію з обмеженим доступом. Необхідно провести аналіз і визначити характеристики небезпечних сигналів:

- періодичне повторення сигналу: є, немає;
- спектральні характеристики сигналу.

Після цього можна приступати безпосередньо до визначення рівнів інформативних ПЕМВ. Тут використовуються такі методи: метод оціночних розрахунків, метод примусової (штучної) активізації; метод еквівалентного приймача.

Метод оціночних розрахунків

Визначаються елементи конструкції обладнання, в яких циркулюють небезпечні сигнали, складаються моделі, проводиться оцінний розрахунок рівня випромінювань. Цей метод добре реалізується при наявності програмного забезпечення для комп'ютера у вигляді експертної системи, що містить банк моделей випромінювачів.

Метод примусової активізації (найчастіше використовується на практиці).

Активізується (програмно або апаратно) канал (один небезпечний ланцюг) еталонним сигналом, який дозволяє ідентифікувати випромінювання, і вимірюються рівні виникаючих ПЕМВ. Для вимірювань за даним методом можуть бути використані вимірювальні приймачі та аналізатори спектра.

Метод еквівалентного приймача

Синтезується приймач для відновлення інформації, що міститься в ПЕМВ. Після калібрування такий приймач може бути використаний для вимірювання рівнів інформаційних випромінювань.

Кожен з методів має свої переваги і недоліки. В даний час найбільш прийнятним для практики методом оцінки рівнів інформативних ПЕМВ являється метод примусової активізації.

Контрольні запитання

1. На які типи, за результатами впливу на інформацію і систему її обробки, підрозділяються загрози.

2. Розказати загальну класифікацію загроз інформації.

3. Що є джерелами утворення природних каналів витоку інформації які утворюються при роботі комп’ютера.

4. Яка сутність пасивних методи захисту інформації.

5. Яка сутність активних методи захисту інформації.

6. Яка сутність активного радіотехнічного маскування.

7. Розказати сутність енергетичного маскування методом “білого шуму”.

8. Які методи використовуються для визначення рівнів інформативних побічних електромагнітних випромінювань.

9. Сутність методу примусової активізації при визначенні рівнів інформативних побічних електромагнітних випромінювань.

10. Які загрози інформації визначаються як “суб’єктивні”?

11. Які загрози інформації визначаються як “об’єктивні”?

12. Сутність методу оціночних розрахунків при визначенні рівня ПЕМВ.

13. Сутність методу еквівалентного приймача при визначенні рівня ПЕМВ.

Лекція № 4

Тема. Матеріально-речовий канал витоку інформації

Особливість цього каналу викликана специфікою джерел і носіїв інформації в порівнянні з іншими каналами. Джерелами і носіями інформації в ньому є суб'єкти (люди) і матеріальні об'єкти (макро і мікрочастинки), які мають чіткі просторові межі локалізації, за винятком випромінювань радіоактивних речовин. Витік інформації в цих каналах супроводжується фізичним переміщенням людей і матеріальних тіл з інформацією за межами контрольованої зони. Для більш чіткого опису розглянутого каналу доцільно уточнити склад джерел і носіїв інформації.

Основними джерелами витоку інформації з матеріально-речового каналу є наступні [3]:

- чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв, що розробляються в ході науково-дослідних і дослідно-конструкторських робіт, що ведуться в організації;

- відходи діловодства та видавничої діяльності в організації, у тому числі використана копіювальний папір, забраковані листи при оформленні документів та їх розмноженні;

- бракована продукція та її елементи;

- відходи виробництва з демаскеруючими речовинами в газоподібному, рідкому і твердому вигляді.

Перенесення інформації в цьому каналі за межі контрольованої зони можливий наступними суб'єктами та об'єктами:

- співробітниками організації;

- повітряними масами атмосфери;

- рідким середовищем;

Ці носії можуть переносити всі види інформації: семантичну і ознаковими, а також демаскуючі речовини.

Семантична інформація міститься в чернетках документів, схем, креслень;

- інформація про видових і сигнальних демаскеруючих ознаках в бракованих вузлах і деталях, в характеристиках радіоактивних випромінювань тощо;

- демаскуючі речовини - в газоподібних, рідких і твердих відходах виробництва.

Приймачі інформації цього каналу досить різноманітні. Це експерти зарубіжної розвідки або конкурента, прилади для фізичного та хімічного аналізу, засоби обчислювальної техніки, приймачі радіоактивних випромінювань та ін [5].

Втрати носіїв з цінною інформацією можливі при відсутності в організації чіткої системи обліку її носіїв. Наприклад, зіпсований співробітником аркуш звіту може бути викинутий їм у кошик для паперу, з якого він буде прибиральницею перенесений в бак для сміття на території організації, а далі при перевантаженні бака або транспортуванні сміття на звалище лист може бути винесений вітром і піднятий перехожим. Звичайно, ймовірність забезпечення випадкового контакту з цим листом зловмисника невелика, але якщо останній активно займається добуванням інформації, то область простору, в якому можливий контакт, значно звужується і ймовірність витоку підвищується.

Для підприємств хімічної, парфумерної, фармацевтичної та інших сфер розробки і виробництва продукції, технологічні процеси яких супроводжуються використанням або отриманням різних газоподібних або рідких речовин, можливе утворення каналів витоку інформації через викиди в атмосферу газоподібних або слив у водойми рідких демаскирующих речовин.

Подібні канали утворюються при появі можливості добування демаскуючих речовин в результаті взяття зловмисниками проб повітря, води, землі, снігу, пилу на листках чагарників і дерев, на траві і квітах в околицях організації.

Залежно від направленя і швидкості вітру демаскуючі речовини в газоподібному вигляді або у вигляді суспендованих твердих частинок можуть поширюватися на відстані в одиниці і десятки км, достатні для безпечного взяття проб зловмисниками. Аналогічне становище спостерігається і для рідких відходів.

Звичайно, концентрація демаскуючих речовин при видаленні від джерела убуває, але при витоку їх протягом деякого часу концентрація може перевищувати допустимі значення за рахунок накопичення демаскирующих речовин в землі, рослинності, підводного флорі і фауні.

Відходи можуть продаватися іншим підприємствам для використання у виробництві іншої продукції, очищатися перед зливом у водойми, знищуватися або піддаватися захороненню на час саморуйнування або розпаду. Останні операції виконуються для високотоксичних речовин, утилізація яких іншими способами економічно недоцільна, і для радіоактивних відходів, які не можна нейтралізувати фізичними або хімічними способами.

Комплексне використання каналів витоку інформації.

Різноманіття розглянутих можливостей витоку інформації надає зловмисникові великий вибір шляхів, способів і засобів добування інформації. На

основі результатів аналізу кожного з розглянутих каналів можна зробити наступні висновки.

1. Витік семантичної інформації можлива за всіма технічними каналами. По можливостях, а отже за загрозою безпеки інформації їх можна проранжувати в наступній послідовності: радіоелектронний, акустичний і оптичний канали. Проте у деяких конкретних умовах можливі інші ранги каналів, наприклад, коли є реальна передумова для спостереження або фотографування документів.

До демаскуючих ознаках об'єктів відносяться:

- ознаки діяльності: рух транспортних машин, звуки, вогні, спалахи, дим, пил;

- здатність відображати і випускати різні випромінювання (електромагнітні, інфрачервоні, теплові), уловлювані спеціальними приладами;

- сліди діяльності: стежки і дороги, залишки виробничих матеріалів, побутове сміття і т.д .;

- характерні обриси (форма), розміри і особливості розташування об'єктів;

- колір поверхні об'єктів, а в деяких випадках і блиск її (блиск стекол, відблиск металу);

- тіні, падаючі від об'єктів, а також тіні на поверхні самих об'єктів.

- ознаки, що характеризують фізичні властивості речовини об'єкта (теплопровідність, електропровідність, структура, твердість і т. Д.);

- ознаки, що характеризують фізичні поля, створювані об'єктами (електромагнітні, радіаційні, акустичні, гравітаційні та ін.);

- ознаки, що характеризують форму, колір, розміри об'єкту і його елементів;

- просторові ознаки, що характеризують як координати об'єкта, так і їх похідні для рухомого об'єкту;

- ознаки, що характеризують наявність певних зв'язків між об'єктами і їх елементами;

- ознаки, що характеризують результати функціонування об'єктів (задимленість, запиленість, сліди об'єкта на грунті, забруднення води і повітря і т. д.).

Виявлення об'єкту проводиться за його демаскуючими ознаками, які діляться на три групи: видові, ознаки діяльності і розташування.

До видових демаскуючих ознак належать фізичні властивості об'єкта (здатність відбивати випромінювання оптичного і радіолокаціонного діапазонів хвиль, випромінювати енергію в тепловому діапазоні) і геометричні властивості (форма, розмір об'єкта та його окремих деталей). Демаскуючі ознаки діяльності проявляються в результаті дій об'єкта (переміщення, зміна навколишнього середовища та ін.). Ознаки розташування характеризуються становищем об'єктів

щодо місцевих предметів. При дешифруванні спостерігач має справу не з самими демаскирующими ознаками, а з носіями первинної інформації про них, які можуть мати різну фізичну основу. Носіями демаскуючих ознак є фізичні поля. Отже, параметри фізичних полів об'єктів і є їх демаскуючими ознаками [6].

Найбільшими потенційними можливостями з добування інформації про видових демаскиуючих ознаках володіє оптичний канал, в якому інформація видобувається шляхом фотографування. Це обумовлено наступними особливостями фотозображення:

- має найвище дозвіл навіть на великій відстані від об'єкта спостереження, наприклад, при детальній фотозйомці з космосу воно досягає 10-15 см на місцевості;

- має найвищу інформаційну ємність, обумовлену максимумом демаскирующих ознак, у тому числі наявністю такого інформативного ознаки як колір;

- забезпечує відносно низький рівень геометричних спотворень.

Інформаційні ємності телевізійних зображень приблизно на порядок нижче фотозображень. Телевізійні зображення мають гірше дозвіл, підвищений рівень яскравості спотворень за рахунок нерівномірності спектрально-характеристик яскравості приладів із зарядним зв'язком, підвищений рівень геометричних спотворень за рахунок додаткових спотворень при формуванні електронного растра.

Зображення в ІЧ-діапазоні володіють ще більш низькими інформаційними параметрами. Крім низької роздільної здатності і великих спотворень для зображень в ІК-діапазоні характерна крайня мінливість яскравості протягом доби.

Однак, як уже зазначалося при розгляді каналів витоку інформації, зображення в кожному з них містить додаткові ознаки за рахунок різної їхньої природи.

Основним каналом здобуття сигнальних демаскуючих ознак є радіоелектронний. У значно меншому обсязі витік інформації про сигнальних демаскирующих ознаках можлива в акустичному каналі [7].

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

- комплексируємі канали доповнюють один одного за своїми можливостями;

- ефективність комлексування підвищується при зменшенні залежності між джерелами інформації та демаскирующими ознаками в різних каналах.

Комплексування каналів витоку інформації забезпечує:

- збільшення ймовірності виявлення і розпізнавання об'єктів за рахунок розширення їх поточних прізнакових структур;

- підвищення достовірності семантичної інформації і точності вимірювання ознак, особливо у разі добування інформації з недостатньо надійних джерел.

Коли виникають сумніви в достовірності інформації, то з метою виключення дезінформації, отримані відомості і дані перепроверяют по іншому каналу.

Класифікація матеріально-речових каналів витоку інформації.

У практиці розвідки широко використовується 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.

Для запобіганню витоку інформації матеріально-речовим каналом використовують технічні, фізичні засоби.

До технічних відносять: найчастіше - технічні системи охорони об’єктів, системи контролю та управління доступом на ОІД.

Контрольні запитання

1. Що є основними джерелами витоку інформації з матеріально-речового каналу?

2. Що являється приймачем інформації матеріально-речового каналу?

3. Що відноситься до демаскуючих ознак об’єктів?

4. Для чого застосовується комплексування матеріально-речових каналів витоку інформації?

5. Що використовується для протидії витоку інформації матеріально-речовим каналом?

Лекція № 5

Тема. Технології захисту акустичної інформації

ПЛАН ЛЕКЦІЇ

1. Критерії захищеності акустичної інформації
2. Пасивні методи захисту інформації
3. Активні методи захисту інформації

1. Критерії захищеності акустичної інформації

Захист мовної інформації є важливим завданням в загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єкта чи установи. Для її перехоплення передбачуваний порушник інформаційної безпеки може використовувати широкий арсенал портативних засобів акустичної мовної розвідки, дозволяють перехоплювати мовну інформацію по прямому акустичному, віброакустичному, оптико-електронному каналам. Як розглянуто у попередньому пункті основними засобами неголосного отримання акустичної інформації є [1, 2, 3]:

- портативна апаратура звукозапису (малогабаритні диктофони, магнітофони та пристрої запису на основі цифрової схемотехніки);
- спрямовані мікрофони;
- акустичні стетоскопи;
- різноманітні закладні пристрої;
- оптико-електронні (лазерні) стетоскопи.

Використання тих чи інших методів і засобів визначається характеристиками об'єкта захисту і апаратурою розвідки, умовами її ведення, а також вимогами, що пред'являються до ефективності захисту акустичної (мовної) інформації. У якості показника оцінки захищеності мовної інформації використовується словесна розбірливість мови (W) на виході каналу витоку інформації [3]. Критерії ефективності захисту акустичної (мовної) інформації багато в чому залежать від цілей, переслідуваних при організації захисту, наприклад:

- приховати смисловий зміст ведення розмови;
- приховати тематику ведення розмови і т.д.

Процес сприйняття мови в шумі супроводжується втратами складових елементів мовного повідомлення. Зрозумілість мовного повідомлення характеризується кількістю правильно прийнятих слів, що відбивають якісну область зрозумілості, яка виражена в категоріях подробиці довідки про

перехоплений розмові, яку зводять «агентом». З практичних міркувань може бути встановлена шкала оцінок якості перехопленого мовного повідомлення:

1. Перехоплене мовне повідомлення містить кількість правильно зрозумілих слів, достатнє для складання докладної довідки про практичний зміст перехопленого розмови.

2. Перехоплене мовне повідомлення містить кількість правильно зрозумілих слів, достатнє лише для складання короткої довідки-анотації, що відбиває предмет, проблему, мету і загальний сенс перехопленого розмови.

3. Перехоплене мовне повідомлення містить окремі правильно зрозумілі слова, що дозволяють встановити предмет розмови.

4. При прослуховуванні перехопленого мовного повідомлення можливо встановити факт наявності мови, але не можна встановити предмет розмови.

Відповідно до проведених досліджень [10] встановлено, що розуміння переданої по каналах зв'язку мови з великим напруженням уваги, перепитав і повтореннями спостерігається при складової розбірливості 20-40%, а при складової розбірливості менше 20% має місце нерозбірливість зв'язного тексту (зрив зв'язку) протягом тривалих інтервалів часу:

Повний захист (конфіденційність забезпечено):

Словесна розбірливість: W < 20%.

Розбірливість фраз: (0%).

Результат: Складові звуки чути, але зрозуміти зміст розмови чи виділити окремі слова неможливо.

Слабкий (недостатній) захист:

Словесна розбірливість: (20% < W <40%).

Результат: Окремі слова стають зрозумілими, можна перехопити загальну тему бесіди.

Перехоплення інформації (захист відсутній):

Словесна розбірливість: (W > 40%).

Розбірливість фраз: понад (60% - 70%).

Результат: Зміст розмови вільно фіксується та документується сторонніми особами.

Таким чином зрив зв'язку буде спостерігатися при словесної чіткості менш ніж 70%. Захист мовної інформації досягається проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням електронних пристроїв перехоплення інформації. 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, у якості показника оцінки якої використовується словесна розбірливість мови *W*.

2. 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 методами:

- пасивні методи захисту (зменшення (ослаблення) рівня мовного сигналу);
- активні методи захисту (збільшення рівня шуму (створення акустичних і вібраційних перешкод)).

Ослаблення акустичних сигналів здійснюється шляхом звукоізоляції приміщень, яка спрямована на локалізацію джерел акустичних сигналів усередині 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 звукопоглинальні матеріали.

Підвищення звукоізоляції стін і перегородок приміщення також досягається установкою на відстані в 6 ... 10 см від них одношарових і багатошарових (частіше подвійних) огороджень. У багатошарових огорожах доцільно підбирати матеріали шарів з різко відрізняються акустичними властивостями (наприклад, бетон — поролон). Для зниження величини вібраційного сигналу використовуються м'які віброізольовані опори, якими розв'язуються один від одного різні огороджувальні конструкції. В якості таких опор застосовують тверду гуму, пробку, свинець. Одним з найбільш слабких звукоізолюючих елементів огороджувальних конструкцій виділених приміщень є двері і вікна. Звукопоглинальна здатність вікон залежить, головним чином, від поверхневої густини скла і ступеня притиснення притворів. Збільшення звукоізолюючої здатності дверей досягається застосуванням ущільнюючих прокладок, оббивкою або облицюванням полотен дверей спеціальними матеріалами. Для захисту інформації в особливо важливих приміщеннях використовуються двері зі звукоізольованим дверним прорізом, виконаному у вигляді тамбура з глибиною не менше 0,5 м При цьому внутрішній простір тамбура має бути оброблено звукопоглинальним матеріалом, полотна дверей обладнані ущільнювачами, а двері оббиті звукопоглиначем із оббивних матеріалів. В особливо важливих приміщеннях використовують спеціальні звукоізолюючі двері. 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.

3. Активні методи захисту інформації

Якщо необхідно розробляти 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. Найпростіші методи отримання білого шуму зводяться до використання шумливих електронних елементів (лампи, транзистори, різні діоди) з посиленням напруги шуму. Більш досконалими є цифрові генератори шуму, які генерують коливання, що представляють собою тимчасової випадковий процес, близький за своїми властивостями до процесу фізичних шумів. Цифрова послідовність двійкових символів в цифрових генераторах шуму являє собою послідовність прямокутних імпульсів з псевдовипадковими інтервалами між ними. Період повторень всієї послідовності значно перевищує найбільший інтервал між імпульсами. Найбільш часто для отримання сигналу зворотного зв'язку застосовуються послідовності максимальної довжини, які формуються за допомогою регістрів зсуву і підсумовуються по модулю За принципом дії всі технічні засоби просторового зашумлення можна розділити на три великі групи [2, 3]:

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

Генератори шуму в мовному діапазоні отримали досить широке поширення в практиці ЗІ. Вони використовуються для захисту від несанкціонованого отримання акустичної інформації шляхом маскування безпосередньо корисного звукового сигналу. Маскування проводиться білим шумом з коригувати спектральної характеристикою. Білий шум - стаціонарний шум (шум характеризується постійністю середніх параметрів: інтенсивності (потужності), розподілу інтенсивності по спектру (спектральна щільність), автокореляційної функції), спектральні складові якого рівномірно розподілені по всьому діапазону задіяних частот. Найбільш ефективним засобом захисту приміщень, призначених для проведення конфіденційних заходів, від знімання інформації через шибки, стіни, системи вентиляції, труби опалення, двері і т.д. є пристрої віброакустичного захисту. Дана апаратура дозволяє запобігти

прослуховування за допомогою дротових мікрофонів, звукозаписної апаратури, радіомікрофонів і електронних стетоскопів, систем лазерного знімання акустичної інформації з вікон і т.д. Протидія прослуховуванню забезпечується внесенням віброакустичних шумових коливань в елементи конструкції будівлі.

Генератор формує білий шум в діапазоні звукових частот. Передача акустичних коливань на огороджувальні конструкції проводиться за допомогою п'єзоелектричних і електромагнітних вібраторів з елементами кріплення. Конструкція і частотний діапазон випромінювачів повинні забезпечувати ефективну передачу вібрації. Віброперетворювачі збуджують шумові віброколивання в огороджувальних приміщеннях, забезпечуючи при цьому мінімальний рівень завадового акустичного сигналу в приміщенні, який практично не впливає на комфортність проведення переговорів. Передбачена в більшості виробів можливість підключення акустичних випромінювачів дозволяє зашумлять вентиляційні канали та дверні тамбури.

Як правило, є можливість плавного регулювання рівня шумового акустичного сигналу. Відмінною особливістю цих засобів є вплив на мікрофонний пристрій і його підсилювач достатньо могутнім ультразвуковим сигналом, що викликає блокування підсилювача або виникнення значних нелінійних спотворень, що призводять, в кінцевому рахунку, 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 спрямованих мікрофонів.

Мікрофони, як відомо, перетворюють енергію звукового сигналу в електричні сигнали. У сукупності зі спеціальними підсилювачами і фільтрами 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. Природно, що методи радіоконтролю, ефективні для пошуку радіозакладок, в даному випадку не мають сенсу. Для захисту від вбудованих і вузько спрямованих мікрофонів рекомендуються такі заходи:

- при проведенні нарад слід обов'язково закривати вікна і двері (найкраще, щоб кімната для наради 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.

Із застосовуваних зараз технічних засобів захисту акустичної інформації можна виділити наступні основні групи:

- генератори акустичного шуму;
- нелінійні локатори;
- скремблери (системи захисту телефонних переговорів);
- детектори мережі 230 В 50 Гц;
- детектори підключень до телефонної лінії;
- комплекси, що забезпечують виконання декількох функцій по "очищенню приміщень".

Завдання технічної контррозвідки ускладнюється тим, що, як правило, невідомо, яке конкретно технічний пристрій контролю інформації застосовано. Тому робота з пошуку і знешкодження технічних засобів спостереження дає обнадійливий результат тільки в тому випадку, якщо вона проводиться комплексно, коли обстежать одночасно всі можливі шляхи витоку інформації. Класифікація пристроїв пошуку технічних засобів підслуховування може бути наступною:

1. Пристрої пошуку активного типу:

- нелінійні локатори (досліджують відгук на вплив електромагнітним полем);
- ретгенметри (просвічують за допомогою рентгенівської апаратури);

2. Пристрої пошуку пасивного типу:

- металошукачі;
- тепловізори;

3) пристрої та системи пошуку по електромагнітному випромінюванню (скануючий приймач, детектор електромагнітного поля);

4). пристрою пошуку по зміні параметрів телефонної лінії (напруги, індуктивності, ємності, добротності);

5). пристрою пошуку по зміні магнітного поля (детектори записуючої апаратури).

Спеціальні приймачі для пошуку працюють передавачів в широкому діапазоні частот називають сканерами. 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. Для захисту приміщень широко використовуються пристрої постановки перешкод. Сигнали перешкоди радіодіапазоні прийнято ділити на загороджувальні і прицільні. Загороджувальна перешкода ставиться на весь широкий діапазон частот, в якому передбачається робота радіопередавача, а прицільна - точно на частоті цього пристрою радіосигналу. Принцип роботи постановника прицільної перешкоди полягає в наступному. Постановник перешкоди працює в автоматичному режимі. Приймач-сканер сканує весь радіодіапазон, а частотомір вимірює частоти виявлених радіопередавачів. Потім пристрій аналізує дані, що надходять і порівнює їх із записаними в пам'ять. При появі сигналів, про які в пам'яті відсутня інформація, видається команда радіопередавачу на постановку прицільної перешкоди. Недоліком таких комплексів є їх висока вартість.

Постановники перешкод інфрачервоного і надвисокочастотного діапазону є складними і дорогими системами. Це пов'язано з тим, що передавачі та приймачі цих діапазонів мають гостру діаграму спрямованості, і, щоб придушити сигнал передавача цих діапазонів, постановник перешкоди повинен точно встановити розташування приймального пристрою, інакше перешкода буде малоефективна. Отже, чим більше спрямованими антенами забезпечені радіомікрофони та їх приймальні пристрої, тим важче поставити проти них перешкоду. Крім того, при тому ж рівні сигналу такі радіолінії мають більшу дальність, що, в свою чергу, ускладнює постановку перешкод.

Найбільш поширеними є постановники перешкод акустичного діапазону з використанням функції створення віброзавад. Це відносно прості й недорогі пристрої, які створюють просторове зашумлення в основному спектрі звукових частот, що забезпечує маскування розмов і знижує ефективність систем прослуховування, і створюють вібраційні завади на будівельних конструкціях та інженерних комунікаціях ОІД (підлога, стелі, стіни, вентиляційні отвори, батареї опалення та ін.

Наприклад прикладом такого приладу є сучасний генератор акустичного та віброакустичного шуму вітчизняної розробки “РІАС-2ГС” рис. 5.1 [11].

Він призначений для захисту об'єктів від витоку конфіденційної інформації акустичними та віброакустичними каналами шляхом створення шумового сигналу в діапазоні частот від 180 Гц до 5,6 кГц.

Комплекс віброакустичного захисту “РІАС-2ГС” має чотири канали формування перешкод, до кожного з яких можуть підключатися вібропетворювачі п'єзоелектричного або електромагнітного типу, а також акустичні системи, що забезпечують перетворення електричного сигналу, який формується приладом, в механічні коливання в огороджувальних конструкціях приміщення, вікон, а також в акустичні коливання повітря.

Максимальна вихідна потужність акустичного та електромеханічного каналу - не менше 10 Вт.

Рис. 5.1 Сучасний генератор акустичного та віброакустичного шуму

Вихідна середньоквадратична напруга акустичного та електромагнітного каналів при мінімальному опорі навантаження 4 Ом - не менше 5 В. Максимальна вихідна потужність п'єзоелектричного каналу - не менше 10 Вт. Вихідна середньоквадратична напруга п'єзоелектричного каналу при максимальній ємності навантаження 0,5 мкФ - не менше 20 В. Прилад забезпечує глибину регулювання окремо низько та високочастотної складових шумового сигналу в робочому діапазоні частот не менше 20 дБ.

Контрольні запитання

1. Назвати основні засоби перехоплення мовної інформації.
2. Що використовується в якості критерію ефективності захисту акустичної інформації?
3. За рахунок чого добиваються зниження розбірливості мови?
4. Чим забезпечується реалізація пасивного методу захисту акустичної інформації?
5. Розказати про активний метод захисту інформації по акустичні каналу.
6. Розказати про пасивні методу захисту інформації по акустичні каналу.
7. Розказати про віброакустичний захист приміщень по акустичному каналу.

Лекція № 6

Тема. Технології захисту інформації в автоматизованих системах від витоку радіоелектронним каналом

ПЛАН ЛЕКЦІЇ

1. Просторове та лінійне зашумлення
2. Фільтрація інформаційних сигналів у електричних колах об’єкту інформаційної діяльності
3. Типи екранувань
4. Заземлення технічних засобів

1. Просторове та лінійне зашумлення

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

Для виключення перехоплення побічних електромагнітних випромінювань використовується просторове зашумлення, а для виключення отримання наведень інформаційних сигналів зі сторонніх провідників і з'єднувальних ліній допоміжних технічних засобів - лінійне зашумлення**.**

До системи просторового зашумлення, що застосовується для створення електромагнітних перешкод, що маскують, пред'являються такі вимоги:

- система має створювати електромагнітні перешкоди у діапазоні частот можливих побічних електромагнітних випромінювань ТЗОІ;
- перешкоди, що створюються, не повинні мати регулярної структури;
- рівень створюваних перешкод (як електричної, так і магнітної складової поля) повинен забезпечити відношення с/ш на межі контрольованої зони менше допустимого значення у всьому діапазоні частот можливих побічних електромагнітних випромінювань ТЗОІ;
- система повинна створювати перешкоди як із горизонтальною, так і з вертикальною поляризацією (тому вибору антен для генераторів перешкод приділяється особлива увага);
- на межі контрольованої зони рівень перешкод, створюваних системою просторового зашумлення, не повинен перевищувати необхідних норм ЕМС.

Мета просторового зашумлення вважається досягнутою, якщо відношення небезпечний сигнал/шум на межі контрольованої зони не перевищує деякого допустимого значення, що вказаного у нормативних документах.

У системах просторового зашумлення переважно використовуються перешкоди типу “білого шуму” або “синфазні перешкоди” [3].

В даний час в основному застосовуються системи просторового шуму, що використовують перешкоди типу “білий шум”, тобто випромінюють широкосмуговий шумовий сигнал (як правило, з рівномірно розподіленим енергетичним спектром у всьому робочому діапазоні частот), що істотно перевищує рівні побічних електромагнітних випромінювань. Такі системи використовуються для захисту широкого класу технічних засобів: електронно-обчислювальної техніки, систем звукопідсилення та звукового супроводу, систем внутрішнього телебачення тощо.

У системах просторового зашумлення в основному використовуються слабоспрямовані рамкові жорсткі та гнучкі антени. Рамкові гнучкі антени виконуються із звичайного дроту і розгортаються у двох-трьох площинах, що забезпечує формування перешкодового сигналу як з вертикальною, так і горизонтальною поляризацією у всіх площинах.

При використанні систем просторового зашумлення необхідно пам'ятати, що поряд з перешкодами засобам розвідки створюються перешкоди та іншим радіоелектронним засобам (наприклад, телебачення, радіозв’язок і т.ін.). Тому при введенні в експлуатацію системи просторового зашумлення, необхідно проводити спеціальні дослідження щодо вимог забезпечення електромагнітної сумісності (ЕМС). Крім того, рівні перешкод, які створює система зашумлення, повинні відповідати санітарно-гігієнічним нормам. Однак норми на рівні електромагнітних випромінювань за вимогами ЕМС істотно суворіші за санітарно-гігієнічні норми. Отже, основну увагу необхідно приділяти виконання норм ЕМС. Просторове зашумлення ефективне як закриття електромагнітного, так й електричного каналів витоку інформації, оскільки перешкодний сигнал при випромінюванні наводиться у сполучних лініях ДТЗ і сторонніх провідниках, які виходять межі контрольованої зони.

Системи лінійного зашумлення застосовуються для маскування наведених небезпечних сигналів у сторонніх провідниках та сполучних лініях ДТЗ, що виходять за межі контрольованої зони. У найпростішому випадку система лінійного зашумлення являє собою генератор шумового сигналу, що формує шумову напругу, що маскує, з заданими спектральними, тимчасовими і енергетичними характеристиками, який гальванічно підключається до лінії (стороннього провідника). На практиці найчастіше подібні системи використовуються для зашумлення ліній електроживлення.

2. Фільтрація інформаційних сигналів у електричних колах об’єкту інформаційної діяльності

Фільтрація інформаційних сигналів - відноситься до пасивних засобів захисту інформації від витоку електричним каналом [3].

Одним із методів локалізації небезпечних сигналів, що циркулюють у технічних засобах та системах обробки інформації, є фільтрація інформаційних сигналів.

У джерелах електромагнітних полів та наведень фільтрація здійснюється з метою запобігання розповсюдженню небажаних електромагнітних коливань за межі пристрою - джерела небезпечного сигналу.

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

Розділові трансформатори. Такі трансформатори повинні забезпечувати розв'язку первинного та вторинного ланцюгів за сигналами наведення. 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 та ємнісних ланцюгів зв'язку між обмотками.

Для зменшення зв'язку обмоток по сигналах наведень часто застосовується внутрішній екран, який виконується у вигляді заземленої прокладки або фольги, що укладається між первинною та вторинною обмотками. За допомогою цього екрана наведення, що діє у первинній обмотці, замикається на землю. Однак електростатичне поле навколо екрана також може спричинити проникнення наведень у вторинний ланцюг.

Розділові трансформатори використовуються для вирішення ряду завдань, у тому числі для:

- поділу по ланцюгах живлення джерел та рецепторів наведення, якщо вони підключаються до тих самих шин змінного струму;

- ослаблення симетричних наведень у ланцюзі вторинної обмотки, зумовлених наявністю асиметричних наведень у ланцюзі первинної обмотки.

Засоби розв'язки та екранування, що застосовуються в розділових трансформаторах, забезпечують максимальне значення опору між обмотками та створюють для наведення шлях з малим опором з первинної обмотки на землю.

Електричні фільтри. В даний час існує велика кількість різних типів фільтрів, що забезпечують ослаблення небажаних сигналів у різних ділянках частотного діапазону. Це фільтри нижніх і верхніх частот, смугові та фільтри, що загороджують. Основне призначення фільтрів - пропускати без значного ослаблення сигнали з частотами, що у робочої смузі частот, і придушувати

(послаблювати) сигнали з частотами, що лежать поза цієї смуги. Для виключення просочування інформаційних сигналів у ланцюзі електроживлення використовуються фільтри нижніх частот. Фільтр нижніх частот (ФНЧ) пропускає сигнали з частотами нижче граничної частоти ($f < fгр$) і пригнічує з частотами вище граничної частоти. Послідовна гілка ФНЧ повинна мати малий опір постійного струму і нижніх частот. Разом з тим, щоб вищі частоти затримувалися фільтром, послідовний опір має зростати з частотою. Цим вимогам задовольняє індуктивність.

Паралельна гілка ФНЧ, навпаки, повинна мати малу провідність для низьких частот для того, щоб струми цих частот не шунтувалися паралельним плечем. Для високих частот паралельна гілка повинна мати велику провідність, тоді коливання цих частот нею шунтуватимуться, і їх струм на виході фільтра послаблюватиметься. Таким вимогам відповідає ємність.

На рис. 6.1 приведена схема однієї R - C ланки ФНЧ для пояснення принципу дії ФНЧ. Згідно з виразом реактивного опору ємності X_C , зі збільшенням у колі електроживлення комп'ютера частоти сигналу (f - ПЕМВ), буде зменшуватися реактивний опір конденсатора. Відповідно схема буде шунтувати наведені ПЕМВ сигнали, або такі що "просочилися" у мережу і таким чином не дозволяючи їм проникнути за межі ОІД.

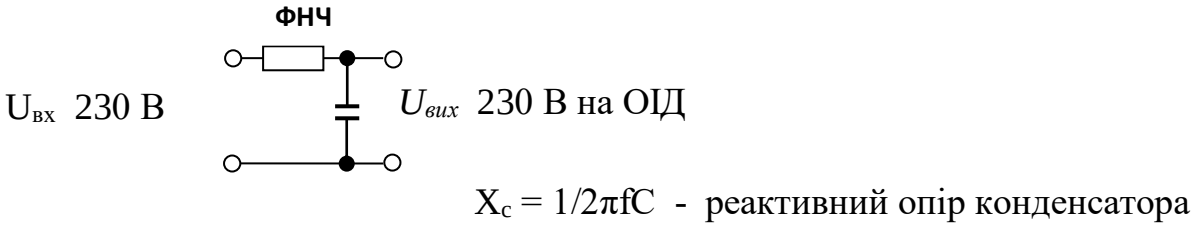

Рис. 6.1 Ланка ФНЧ

На рис. 6.2 [12] приведено вигляд фільтра мережевого перешкододавлюючого М 7, який запобігає витоку інформації з ланцюгів електроживлення, а також захищає засоби оргтехніки від зовнішніх перешкод. Фільтр М 7 послаблює будь-які сигнали в діапазоні 0,1 - 1,8 ГГц з ефективністю 60 дБ і відповідно не пропускає інформативні сигнали, що виникають при роботі засобів оргтехніки.

Більш складні багатоланкові ФНЧ (Чебишева, Баттерворта, Бесселя тощо) конструюють з урахуванням поєднань різних одиничних ланок таких як показано на рис. 6.1.

Основні вимоги до захисних фільтрів полягають у наступному:

- величини робочої напруги та струму фільтра повинні відповідати напрузі та струму фільтрованого ланцюга;

- величина ослаблення небажаних сигналів у діапазоні робочих частот має бути не меншою за необхідну;

- ослаблення корисного сигналу у смузі прозорості фільтра має бути незначним;

- габарити та маса фільтрів повинні бути мінімальними;

- фільтри повинні забезпечувати функціонування за певних умов експлуатації (температура, вологість, тиск) та механічних навантажень (удари, вібрація тощо);

- конструкції фільтрів повинні відповідати вимогам техніки безпеки.

Рис. 6.2 Зовнішній вигляд фільтру низьких частот для живлення ОІД

До фільтрів ланцюгів живлення поряд із загальними висуваються такі додаткові вимоги:

- загасання, що вноситься такими фільтрами в ланцюги постійного струму або змінного струму основної частоти, має бути мінімальним (наприклад, 0,2 дБ і менше) і мати велике значення (більше 60 дБ) у смузі придушення, яка в залежності від конкретних умов може бути досить широкій (до 10 ГГц);

- мережеві фільтри повинні ефективно працювати при сильних струмах, що виходять, високих напругах і високих рівнях потужності проходять і затримуваних електромагнітних коливань;

Наприклад, фільтри серії ФСПК-100 (200), що використовуються на практиці, призначені для встановлення в лініях електроживлення частотою 50 Гц і напругою 230/400 В. Максимальний робочий струм становить 100 (200) А. В - діапазоні частот від 0,02 до 1000 МГц фільтри забезпечують загасання сигналу щонайменше 60 дБ.

3. Типи екранувань

Функціонування будь-якого технічного засобу інформації пов'язане з протіканням по його струмопровідним елементам електричних струмів різних частот і утворенням різниці потенціалів між різними точками його електричної схеми, які породжують магнітні та електричні поля, звані побічними електромагнітними випромінюваннями.

Побічні електромагнітні випромінювання технічного засобу обробки інформації є причиною виникнення електромагнітних та параметричного акустичного каналів витоку інформації, а також можуть стати причиною виникнення наведення інформаційних сигналів у сторонніх струмопровідних лініях та конструкціях. Тому зниженню рівня побічних електромагнітних випромінювань приділяється велика увага.

Ефективним методом зниження рівня ПЕМВ є екранування їх джерел.

Розрізняють такі способи екранування:

- електростатичне;
- магнітостатичне;
- електромагнітне.

Електростатичне та магнітостатичне екранування засновані на замиканні екраном (що володіє в першому випадку високою електропровідністю, а в другому - магнітопровідністю) відповідно електричного та магнітного полів.

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

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

Екрануюча дія металевого листа істотно залежить від якості з'єднання екрана з корпусом приладу та частин екрану один з одним. Особливо важливо не мати з'єднувальних дротів між частинами екрану та корпусом.

У діапазонах метрових і більш коротких довжин хвиль з'єднувальні провідники завдовжки кілька сантиметрів можуть різко погіршити ефективність екранування. На ще більш коротких хвилях дециметрового та сантиметрового діапазонів сполучні провідники та шини між екранами неприпустимі.

Вузькі щілини та отвори в металевому екрані, розміри яких малі в порівнянні з довжиною хвилі, практично не погіршують екранування електричного поля. Зі збільшенням частоти ефективність екранування знижується. Основні вимоги до електричних екранів можна сформулювати таким чином:

- конструкція екрана повинна вибиратися такою, щоб силові лінії електричного поля замикалися на стінки екрана, не виходячи за межі;

- в області низьких частот (при глибині проникнення (σ) більше товщини (d), тобто при σ>d) ефективність електростатичного екранування практично визначається якістю електричного контакту металевого екрана з корпусом пристрою і мало залежить від матеріалу екрану та його товщини;

- в області високих частот (при d<σ) ефективність екрану, що працює в електромагнітному режимі, визначається його товщиною, провідністю та магнітною проникністю.

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

Основні вимоги до магнітостатичних екранів можна звести до наступних:

- магнітна проникність μ матеріалу екрана має бути можливо вищою. Для виготовлення екранів бажано застосовувати магнітом'які матеріали з високою магнітною проникністю (наприклад, пермалою);

- збільшення товщини стінок екрану призводить до підвищення ефективності екранування, проте при цьому слід брати до уваги можливі конструктивні обмеження за масою та габаритами екрану;

- стики, розрізи та шви в екрані повинні розміщуватись паралельно лініям магнітної індукції магнітного поля. Їх кількість має бути мінімальною;

- Заземлення екрану не впливає на ефективність магнітостатичного екранування.

Ефективність магнітостатичного екранування підвищується під час застосування багатошарових екранів.

Екранування високочастотного магнітного поля засноване на використанні магнітної індукції, що створює в екрані змінні вихрові індукційні струми (струми Фуко). Магнітне поле цих струмів усередині екрану буде спрямоване назустріч збуджувальному полю, а за його межами - в той же бік, що й збуджуюче поле. Результуюче поле виявляється ослабленим усередині екрану та посиленим поза ним. Вихрові струми в екрані розподіляються нерівномірно за його перерізом (товщиною). Це викликається явищем поверхневого ефекту, сутність якого полягає в тому, що змінне магнітне поле слабшає принаймні проникнення в глиб металу, так як внутрішні шари екрануються вихровими струмами, що циркулюють у поверхневих шарах.

Завдяки поверхневому ефекту щільність вихрових струмів та напруженість змінного магнітного поля у міру заглиблення в метал падає по експонентному закону.

Ефективність магнітного екранування залежить від частоти та електричних властивостей матеріалу екрану. Чим нижче частота, тим слабше діє екран, тим більшої товщини доводиться його робити для досягнення одного і того ж екрануючого ефекту. Для високих частот, починаючи з діапазону середніх хвиль, екран з будь-якого металу завтовшки 0,5...1,5 мм діє дуже ефективно. При виборі товщини та матеріалу екрану слід враховувати механічну міцність, жорсткість, стійкість проти корозії, зручність стикування окремих деталей та здійснення між ними перехідних контактів з малим опором, зручність паяння, зварювання та ін.

Для частот вище 10 МГц мідна і тим більше срібна плівка завтовшки більше 0,1 мм дає значний ефект, що екранує. Тому на частотах вище 10 МГц цілком допустимо застосування екранів із фольгованого гетинаксу або іншого ізоляційного матеріалу з нанесеним на нього мідним або срібним покриттям.

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

На високих частотах використовується виключно **електромагнітне** екранування. Дія електромагнітного екрана заснована на тому, що високочастотне електромагнітне поле послаблюється ним же створеним (завдяки вихровим струмам, що утворюється в товщі екрана) полем зворотного напрямку.

Теорія та практика показують, що з точки зору вартості матеріалу та простоти виготовлення переваги на стороні екранованого приміщення з листової сталі. Однак при застосуванні сітківки можуть значно спроститися питання вентиляції та освітлення приміщення. У зв'язку з цим сітчасті екрани знаходять широке застосування.

Металеві листи або полотнища сітки повинні бути електрично з'єднані по всьому периметру. Для суцільних екранів це може бути здійснено електрозварюванням або паянням. Шов електрозварювання або паяння повинен бути безперервним для того, щоб отримати цільнозварну конструкцію екрана.

Для сітчастих екранів придатна будь-яка конструкція шва, що забезпечує хороший електричний контакт між сусідніми полотнищами сітки не рідше ніж через 10...15 мм Для цієї мети може застосовуватися паяння або точкове зварювання.

Також екрануванню підлягають і монтажні дроти та сполучні лінії. Щоб зменшити рівень ПЕМВ, необхідно ретельно виконувати з'єднання оболонки дроту (екрана) з корпусом апаратури. Підключення оболонки повинно

здійснюватися шляхом безпосереднього контакту (найкраще шляхом паяння чи зварювання) із корпусом.

На низьких частотах доводиться використовувати складніші схеми екранування - коаксіальні кабелі з подвійним обплетенням (тріаксіальні кабелі).

На вищих частотах, коли товщина екрана значно перевищує глибину проникнення поля, потреба у подвійному екрануванні відпадає. У цьому випадку зовнішня поверхня відіграє роль електричного екрану, а по внутрішній поверхні протікають зворотні струми. Довжина екранованого монтажного дроту повинна бути менше чверті довжини найкоротшої хвилі спектра сигналу, що передається по дроту. При використанні більш довгих ділянок екранованих проводів необхідно мати на увазі, що в цьому випадку екранований провід слід розглядати як довгу лінію, яка, щоб уникнути спотворень форми сигналу, що передається повинна бути навантажена на опір, рівне хвильовому

Екрануватися можуть не лише окремі блоки (вузли) апаратури та їх з'єднувальні лінії, а й приміщення загалом.

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

- струмопровідні лакофарбові покриття або струмопровідні шпалери;
- штори із металізованої тканини;
- металізоване скло (наприклад, з двоокису олова), що встановлюється в металеві або металізовані рами.

У приміщенні екрануються стіни, двері та вікна. При зачиненні дверей повинен забезпечуватись надійний електричний контакт зі стінками приміщення (з дверною рамою) по всьому периметру не рідше ніж через 10...15 мм. Для цього може бути використана пружинна гребінка з фосфористої бронзи, яку зміцнюють по всьому внутрішньому периметру дверної рами. Вікна повинні бути затягнуті одним або двома шарами мідної сітки з коміркою не більше 2х2 мм, причому відстань між шарами сітки має бути не менше ніж 50 мм. Обидва шари сітки повинні мати хороший електричний контакт зі стінками приміщення (з рамою) по всьому периметру. Сітки зручніше робити знімними та металеве обрамлення знімної частини також повинно мати пружні контакти у вигляді гребінки з фосфористої бронзи. Розміри екранованого приміщення вибирають виходячи з його призначення та вартості. Зазвичай екрановані приміщення будують площею 6...8 м^2 при висоті 2,5...3 м

4. Заземлення технічних засобів

Необхідно пам'ятати, що екранування ТЗОІ та з'єднувальних ліній ефективне лише при правильному їх заземленні. Тому однією з найважливіших умов захисту ТЗОІ є правильне заземлення цих пристроїв.

Нині існують різні типи заземлень. Найчастіше використовуються одноточкові, багатоточкові та комбіновані (гібридні) схеми.

Одноточкова послідовна схема заземлення найпростіша (рис. 6.3). Однак їй притаманний недолік, пов'язаний з протіканням зворотних струмів різних ланцюгів по спільній ділянці ланцюга, що заземлює. Внаслідок цього можлива поява небезпечного сигналу в сторонніх ланцюгах.

В одноточковій паралельній (радіальній) схемі заземлення (рис. 6.4) цього недоліку немає. Однак така схема вимагає великої кількості протяжних заземлюючих провідників, через що може виникнути проблема із забезпеченням малого опору заземлення ділянок ланцюга. Крім того, між заземлюючими провідниками можуть виникати небажані зв'язки, які створюють декілька шляхів заземлення для кожного пристрою. В результаті в системі заземлення можуть виникнути зрівняльні струми та з'явитися різниця потенціалів між різними пристроями.

Рис. 6.3 Одноточкова послідовна схема заземлення

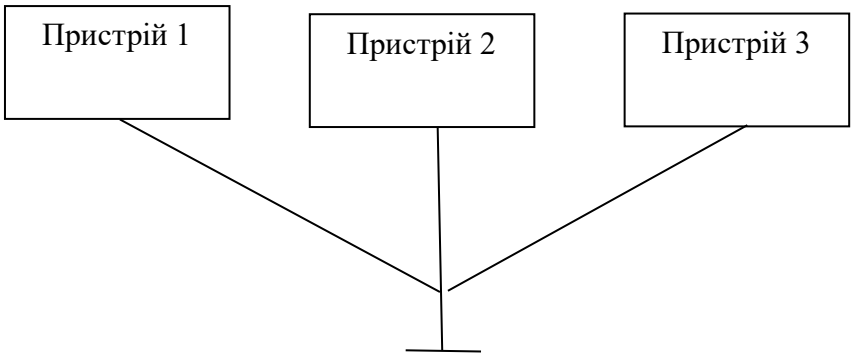

Рис. 6.4 Одноточкова паралельна (радіальна) схема заземлення

Багатоточкова схема заземлення (рис. 6.5) вільна від недоліків, властивих одноточковій схемі. У цьому випадку окремі пристрої та ділянки корпусу індивідуально заземлені.

Як правило, одноточкове заземлення застосовується на низьких частотах при невеликих розмірах пристроїв, що заземлюються, і відстанях між ними менше *0,5 λ*

На високих частотах при великих розмірах пристроїв, що заземлюються, і значних відстанях між ними використовується багатоточкова система заземлення.

Основні вимоги до системи заземлення полягають у наступному:

- система заземлення повинна включати загальний заземлювач, заземлюючий кабель, шини та дроти, що з'єднують заземлювач з об'єктом;

- опори заземлюючих провідників, а також земляних шин мають бути мінімальними;

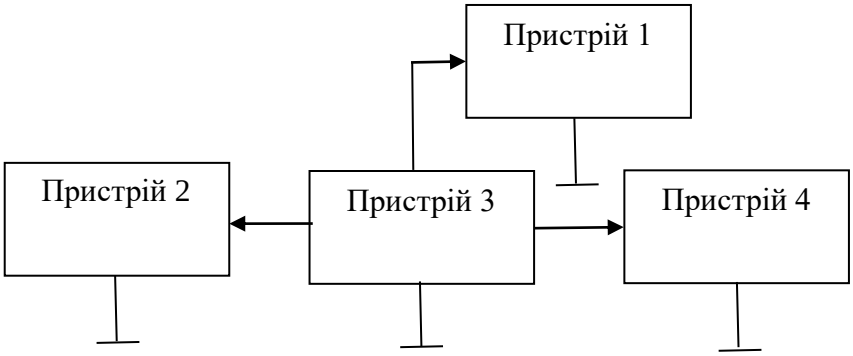

Рис. 6.5 Багатоточкова схема заземлення

- кожен елемент, що заземляється, повинен бути приєднаний до заземлювача або до заземлюючої магістралі за допомогою окремого відгалуження.

- послідовне включення до заземлюючого провідника кількох елементів забороняється;

- у системі заземлення повинні бути замкнуті контури, утворені з'єднаннями або небажаними зв'язками між сигнальними ланцюгами і корпусами пристроїв, між корпусами пристроїв і землею;

- слід уникати використання загальних провідників у системах екрануючих заземлень, захисних заземлень та сигнальних ланцюгів;

- якість електричних з'єднань у системі заземлення має забезпечувати мінімальний опір контакту, надійність та механічну міцність контакту в умовах кліматичних впливів та вібрації;

- контактні сполуки повинні виключати можливість утворення оксидних плівок на поверхнях, що контактують, і пов'язаних з цими плівками нелінійних явищ;

- контактні з'єднання повинні унеможливлювати утворення гальванічних пар для запобігання корозії в ланцюгах заземлення;

- забороняється використовувати як заземлюючий пристрій нульові фази електромереж, металоконструкції будівель, що мають з'єднання із землею, металеві оболонки підземних кабелів, металеві труби систем опалення, водопостачання, каналізації тощо.

Опір заземлення визначається головним чином опором розтікання струму землі. Величину цього опору можна значно знизити за рахунок зменшення перехідного опору між заземлювачем та ґрунтом шляхом ретельного очищення перед укладанням поверхні заземлювача та утрамбовуванням навколо нього ґрунту, а також підсипкою кухонної солі. Таким чином, величина опору заземлення в основному визначатиметься опором ґрунту. з'єднання в одній точці.

При підвищених вимогах до величини опору заземлення (опір заземлення технічного засобу обробки інформації не повинен перевищувати 4 Ом) застосовують багаторазове заземлення, що складається з ряду одиночних симетрично розташованих заземлювачів, з'єднаних між собою. На практиці найчастіше як заземлювач застосовують:

- стрижні з металу, що мають високу електропровідність, занурені в землю та з'єднані з наземними металоконструкціями засобів технічного засобу обробки інформації;

- сіткові заземлювачі, виготовлені з елементів з високою електропровідністю та занурені в землю (служать як доповнення до заземлюючих стрижнів).

При необхідності влаштування високочастотного заземлення потрібно враховувати не тільки геометричні розміри заземлювачів, їх конструкцію та властивості ґрунту, а й довжину хвилі високочастотного випромінювання. Сумарний високочастотний опір заземлення складається з високочастотного опору магістралі заземлення (проводу, що йде від заземлюваного пристрою до поверхні землі) і високочастотного опору самого заземлювача (проводу, металевого стрижня або листа, що знаходиться в землі). Величина заземлення переважно визначається не опором заземлення, а опором заземлюючої магістралі. Для зменшення останнього слід прагнути насамперед зменшення індуктивності заземлюючої магістралі, що досягається за рахунок зменшення її довжини і виготовлення магістралі у вигляді стрічки, що володіє в порівнянні з проводом круглого перерізу меншою індуктивністю.

Найбільш придатними для заземлювачів є труби, що дозволяють досягти глибоких і найбільш вологих шарів землі, що мають найбільшу провідність і не підсихають або промерзають. Однак тут необхідно враховувати, що із зменшенням опору ґрунту зростає корозія металу.

Заземлювачі слід з'єднувати між собою шинами з допомогою зварювання. Перетин шин та магістралей заземлення за умов механічної міцності та отримання достатньої провідності рекомендується брати не менше (24 х 4) мм^2

Провідник, що з'єднує заземлювач із контуром заземлення, повинен бути лудженим для зменшення гальванічної корозії, а з'єднання повинні бути захищені від впливу вологи. Магістралі заземлення поза будівлею необхідно прокладати на глибині близько 1,5 м, а всередині будівлі - стіною або спеціальними каналами таким чином, щоб їх можна було зовні оглядати. З'єднують магістралі із заземлювачем лише за допомогою зварювання.

Контрольні запитання

1. Для чого застосовується заземлення технічних засобів обробки інформації?
2. Які способи екранування використовуються на практиці?
3. Що розуміється під електростатичним екрануванням?
4. Що розуміється під магнітостатичним екрануванням?
5. Що розуміється під електромагнітним екрануванням?
6. Для чого застосовується заземлення технічних засобів? Що використовується як заземлювач?
7. Дати характеристику одноточкову послідовну схему заземлення.
8. Дати характеристику одноточковій паралельній схемі заземлення.
9. Дати характеристику багатоточковій схемі заземлення.
10. Які основні вимоги до системи заземлення?
11. Який опір заземлення технічних засобів на ОІД повинен бути згідно нормативних документів ТЗІ?
12. Чиможна використовувати сторонні провідники, батареї опалення для заземлення?
13. Пояснити пристрій, принцип дії розподільчого трансформатора. Для вирішення яких завдань використовується?
14. Для чого застосовуються завадові ФНЧ? Які основні вимоги до них.

Лекція № 7

Тема. Технології захисту інформації від витоку матеріально-речовим каналом

ПЛАН ЛЕКЦІЇ

1. Склад технічної системи охорони
2. Структура типових варіантів побудови комплексів ТЗОС
3. Класифікація чутливих елементів засобів виявлення

1. Склад технічної системи охорони

У загальному вигляді технічна система охорони включає в себе наступні засоби (рис. 7.1) [3]:

- 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;

Рис. 7.1 Склад технічної системи охорони об’єкту

- 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.).

2. Структура типових варіантів побудови комплексів ТЗОС визначається розподілом логічної обробки інформації від ЗВ і апаратурою ППКОП, а також способом зв'язку між ними і ЗВ. На вибір варіанту структури побудови комплексу головним чином роблять вплив наступні чинники;

- якісний і кількісний склад обслуговуваних ЗВ, концентратори, ППКОП і ін;

- ступінь централізації управління ППКОП;

- структурні особливості об'єктів, що охороняються;

-чинники вартості і надійності.

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

Радіальний (променевий) безконцентраторний (рис. 7.2).

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;

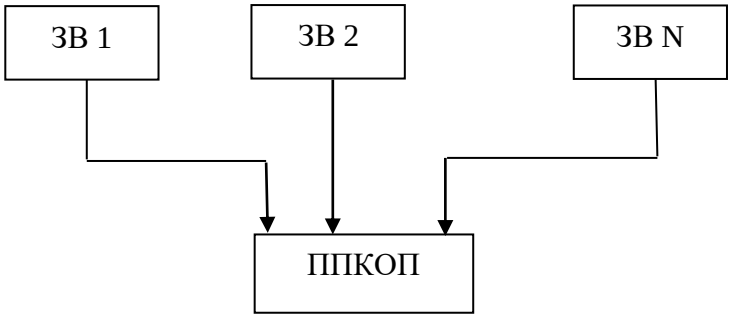

Рис. 7.2 Радіальне (променеве) безконцентраторне з'єднання станційної апаратури із ЗВ

- несправності, що виникають в лініях зв'язку ЗВ і вхідних ланцюгах ППКОП, впливають на працездатність тільки окремого каналу сигналізації, що при відповідній організації охорони не впливає на функціонування всього комплексу ТЗОС;

- значний об'єм і розгалуженість кабельних ліній.

Шлейфовий (магістральний) без концентраторів (рис. 7.3) **і з концентраторами** (рис. 7.4).

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.

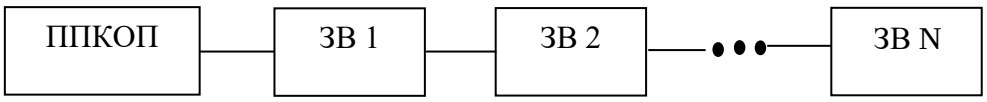

Рис. 7.3 Шлейфове (магістральне) без концентраторів
з'єднання ППКОП із ЗВ

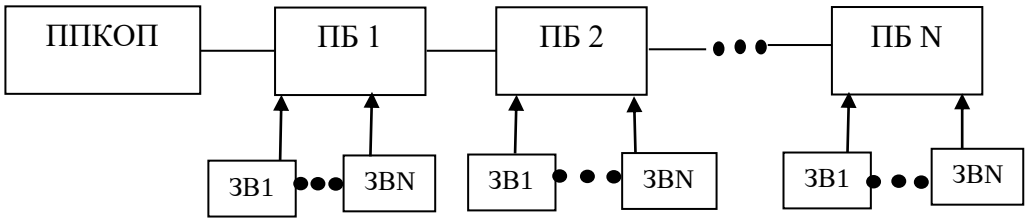

Рис. 7.4 Шлейфове (магістральне) з концентраторами
з'єднання ППКОП з ПБ і ЗВ

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).

Вибір структури побудови комплексу ТЗОС.

При виборі структури побудови комплексу ТЗОС і відповідної апаратури 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 із ППКОП, а для комплексів більшої ємкості - шлейфова з концентраторами. При цьому обробка інформації повинна здійснюватися переважно в концентраторах, об'єднаних із ППКОП по шинній структурі (локальній обчислювальній мережі).

Відмітною особливістю побудови комплексів технічних систем охорони, що містять багато типів ЗВ, є способи адаптації ТСО до конкретних типів контрольованих нею ЗВ. При сполученні ЗВ і ППКОП необхідно погоджувати наступні стикувальні параметри:

- напруга електроживлення ЗВ (якщо воно потрібне);

- час нестійкого стану вихідних контактів ЗВ після подачі на нього напруги електроживлення (час перехідних процесів ЗВ);

- тип дистанційної перевірки працездатності ЗВ.

З метою здійснення контролю за діями оператора по управлінню комплексом ТЗОС і для зручності оперативної роботи до складу комплексу вводиться апаратура зберігання (архівації) і документування інформації. Найбільше розповсюдження отримали накопичення інформації в спеціальному оперативному запам’ятовуючому пристрої або на жорсткому диску комп’ютера з можливістю виведення інформації на букво-цифровий індикатор і\ або її розпечатування.

Проте введення до складу комплексу пристроїв документування вимагає передбачати блоки автоматики, призначені для логічної обробки і підготовки сигналів управління блоками цифро-друкуючого пристрою.

3. Класифікація чутливих елементів засобів виявлення

В попередніх розділах ми розглянули можливі шляхи і способи проникнення порушника на об'єкт охорони. Очевидно, при своєму русі людина-порушник залишає безліч різноманітних слідів свого руху і/або перебування, які можуть бути зафіксовані (а при необхідності зміряні) різними приладами. 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, кватирки; іноді вимушений вирізувати і/або вибивати стекла, або пробляти отвори і проломи в стелях, підлозі або стінах. Усередині приміщення він пересуває предмети, обстановку, намагається розкрити металеві шафи або сейфи, фотографувати документи або вироби. Для виконання цих дій він може мати з собою фотоапаратуру, різний інструмент, а також зброю або вибухові речовини. 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 надвисоких частот. Застосування механічного інструменту для відкриття дверей і металевих шаф, створення проломів і отворів в стінах і підлогах приміщень супроводжується 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.

Типові підходи до класифікації засобів виявлення і технічних засобів охорони. Як було сказано раніше, основу комплексу технічних засобів охорони складають: засоби виявлення; система збору, обробки, відображення і документування інформації (ППКОП); допоміжні засоби і пристрої (блоки резервного електроживлення, і ін..).

Взагалі засоби виявлення класифікують за наступними ознаками [3]:

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;

- рівень освітленості і ін..;

- 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.

Створення рубежів охорони.

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. Такі рубежі (або зони безпеки) повинні розташовуватися послідовно - від огорожі навколо території об'єкту до головного, особливо важливого приміщення, такого як сховище цінностей і інформації, вибухонебезпечних матеріалів, зброї і інші. (рис. 7.5).

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 погроз подадуть сигнал тривоги, а отже, у співробітників охорони залишиться більше часу для визначення причин тривоги і організації ефективного захисту і ліквідації загрози.

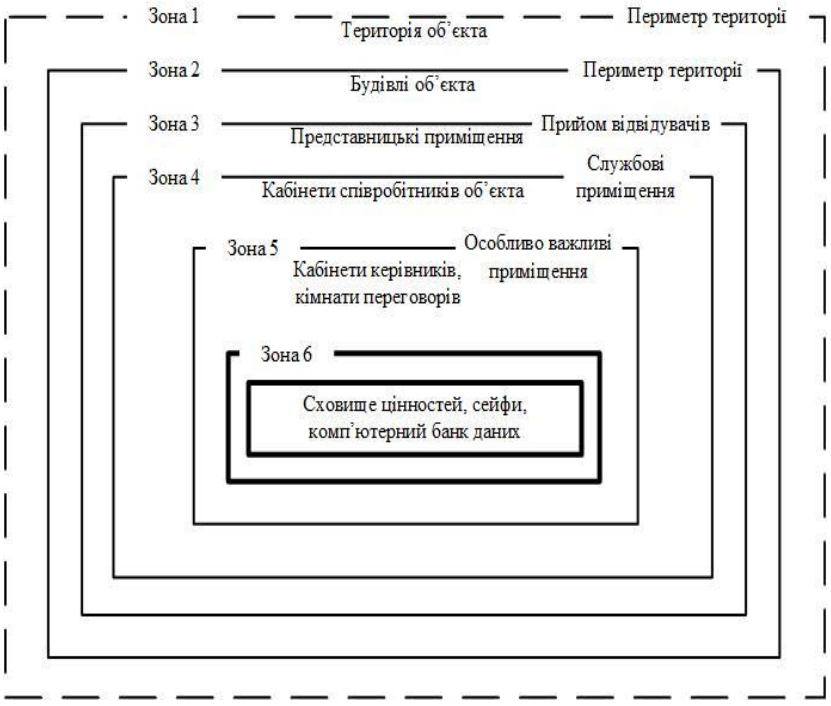

Рис. 7.5 Принцип рубіжності

Основу системи захисту складають технічні засоби виявлення, відбиття і ліквідації наслідків. Охоронна сигналізація і охоронне телебачення, наприклад, відносяться до засобів виявлення погроз. Огорожі навколо території об'єкту - це

засоби відбиття несанкціонованого проникнення на територію; посилені двері, стіни і стелі сейфової кімнати захищають від стихійних лих і аварій, а крім того, до певної міри служать захистом і від підслуховування і вторгнення.

Обов'язковою на ОІД є пожежна сигналізація, яка є більш розгалуженою, ніж інші види і зазвичай охоплює майже всі приміщення будівлі.

Пожежна і охоронна сигналізації по своїй побудові і вживаній апаратурі мають багато загального - канали зв'язку, прийом і обробка інформації, подача тривожних сигналів і ін. З цієї причини в сучасних системах захисту ці типи засобів сигналізації іноді об'єднуються в єдину систему охоронно-пожежної (ОП) сигналізації.

Контроль і управління ОП сигналізацією здійснюються з центрального поста охорони, на якому встановлюється відповідна стаціонарна апаратура. Склад і характеристики цієї апаратури залежать від важливості об'єкту, складності і розгалуженості системи сигналізації.

Критерієм ефективності і досконалості апаратури ОП сигналізації є зведення до мінімуму числа помилок і помилкових спрацьовувань. Наприклад, для особливо важливих об'єктів бажано, щоб вірогідність виявлення ЗВ була близька до 0.98; напрацювання на помилкове спрацьовування - до 2500 годин (для пасивних) і до 3500 годин (для активних).

Каналами зв'язку в системі ОП сигналізації можуть бути спеціально прокладені дротяні лінії, телефонні лінії об'єкту, телеграфні лінії і радіоканали. Енергопостачання системи охоронної сигналізації обов'язково резервується.

Для вирішення завдань оснащення периметра якого-небудь об'єкту технічними засобами охоронної сигналізації заздалегідь слід знати відповіді на питання:

1. Яка протяжність периметра.

2. Вид наявної загорожі (її параметри, матеріал).

3. Кількість наявних воріт, хвірток, їх розміри, матеріал.

4. Найближча відстань від рубежу, що охороняється, до приміщення охорони, до найближчої до периметра будівлі.

5. Наявність застав (труби, кабелі).

6. Розмір зони відчуження усередині периметра, наявність кущів і/або дерев в зоні відчуження.

7. Необхідність скритності засобів виявлення (або відсутність такої необхідності).

8. Необхідна точність виявлення порушника на контурі периметра (3 м, 10 м).

9. Необхідна кількість рубежів охорони (периметр, підходи до будівель), режими охорони: цілодобовий, в міру необхідності, N-часової.

10. Необхідність блокування: перелазу через огорожу, руйнування огорожі, підкопу під огорожу.

11. Наявність в даний час (тобто на момент попереднього аналізу об'єкту охорони) яких-небудь засобів виявлення, станційної апаратури в приміщенні служби охорони - системи збору і обробки інформації.

12. Які витрати може дозволити собі Замовник на вирішення завдань оснащення об'єкту (зокрема периметра) технічними засобами охоронної сигналізації і системою збору і обробки інформації.

13. У які терміни потрібне проведення такої роботи.

14. Необхідний план об'єкту (ескіз), параметри по висоті будівель.

Приведений перелік питань - мінімально необхідний з позицій попереднього аналізу, але далеко не повний з позицій системного підходу.

Об'єктивна необхідність побудови високоефективних систем безпеки об'єктів в умовах різкого загострення криміногенної обстановки привела до розробки наукоємних інтегрованих систем безпеки (ІСБ). ІСБ по суті націлена на реалізацію ідей системної концепції забезпечення комплексної безпеки об'єкту з паралельним (інтегрованим із завданнями забезпечення безпеки) вирішенням завдань автоматизації управління широкою гаммою систем життєзабезпечення об'єкту, як то: енергопостачанням, вентиляцією, опалюванням, водопостачанням, ліфтовим устаткуванням, кондиціонуванням і ін.

Серед функцій, обов'язкових для виконання в контурі ІСБ, слід вважати:

- контроль за великою кількістю приміщень із створенням декількох рубежів захисту (ІСБ розробляється тільки для великих об'єктів і будівель);

- ієрархічний доступ співробітників і відвідувачів в приміщення з чітким розмежуванням повноважень по праву доступу в приміщення за часом доби і по днях тижня;

- ідентифікацію і аутентифікацію особи людини, що перетинає рубіж контролю;

- накопичення документальних матеріалів для використання їх при розгляді і аналізі подій;

- оперативний (автоматизований) інструктаж працівників охорони про порядок дій в різних штатних і нештатних ситуаціях шляхом автоматичного виводу на екран монітора інструкцій в потрібний момент;

- забезпечення повної інтеграції систем відеоспостереження, сигналізації, моніторингу доступу, сповіщення, зв'язку між персоналом СБ (О), персоналом служби пожежної безпеки, персоналом служб життєзабезпечення об'єкту і ін.;

- забезпечення взаємодії постів охорони і органів правопорядку при несенні охорони і у разі відповідних подій;

- стеження за точним виконанням персоналом охорони своїх службових обов'язків.

Виходячи з викладеного раніше ясно, що складовими частинами ІСБ (укрупнено) мають бути:

- мережі ЗВ, що забезпечують отримання максимально повної інформації зі всього простору, що знаходиться у полі зору служби безпеки і що дозволяє відтворювати на центральному пульті спостереження і управління всесторонню об'єктивну картину стану приміщень, всієї території об'єкту і працездатності всієї апаратури і устаткування, включеного в контур ІСБ;

- виконавчі пристрої, здатні при необхідності діяти автоматично або по команді оператора;

- пункти контроля і управління системою відображення інформації, через яких операторів можливо стежити за роботою всієї системи в межах своїх повноважень;

- комунікації, по яких здійснюється обмін інформацією між елементами системи і операторами.

При цьому важлива наявність можливості оперативного програмування (перепрограмування) функцій ІСБ. Це дозволяє ефективно протидіяти таким хитруванням зловмисника як:

- переривання каналів передачі тривоги;

- нейтралізація частини системи людьми, що мають доступ до її елементів;

- проникнення з сигналом тривоги і знищення потім інформації про подію (змова)/

Контрольні запитання

1. Що складає основу комплексу технічних засобів охорони?
2. Як класифікуються засоби виявлення за призначенням?
3. Як класифікуються засоби виявлення по виду контрольованої зони?
4. Як класифікуються засоби виявлення за способом приведення в дію?
5. Як класифікуються засоби виявлення за фізичним принципом дії?
6. Як класифікуються засоби виявлення по конструктивному виконанню?
7. Як класифікуються засоби виявлення по дальності дії?
8. Які основні ТТХ розглядають при розробці нових ЗВ?
9. Які основні компоненти: виділяються в структурі технічних засобів охорони?
10. Що є критерієм ефективності і досконалості апаратури охоронно-пожежної сигналізації?

Лекція № 8

Тема. Технології виявлення спроб проникнення порушника інформаційної безпеки на ОІД

ПЛАН ЛЕКЦІЇ

1. Магнітоконтактний сповіщувач
2. Пасивний інфрачервоний сповіщувач
3. Сповіщувачі розбиття скла

1. Магнітоконтактний сповіщувач

Магнітоконтактні сповіщувачі (МКС) - це найбільш простий, дешевий і в той же час досить надійний вид сповіщувачів, що використовуються в системах охоронної сигналізації. Згадані переваги разом з малими габаритами і простотою встановлення призвели до широкого використання МКС. Основою МКС є контакти, керовані магнітним полем. Основне призначення таких сповіщувачів - фіксація моменту відкривання дверей, вікон або аналогічних конструктивних елементів, а також зсуву предметів [3].

Магнітоконтактний сповіщувач містить у собі два основних елементи. Перший елемент - це геркон (рис. 8.1), що складається з герметичної колби 1, у якій знаходяться пластини 2 з контактами, які мають малий опір. До пластин під'єднанні провідники 3, 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 4 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.

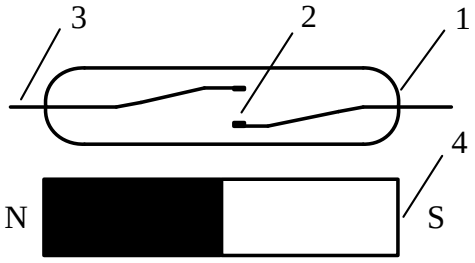

Рис. 8.1 Основні елементи магнітоконтактного сповіщувача

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

Основні параметри магнітоконтактних сповіщувачів/

Робочий зазор. Робочий зазор визначає мінімальну відстань, на якій відбувається замикання контактів геркона (рис. 8.2).

Деякі МКС мають збільшений робочий зазор, що дає можливість встановлювати їх на конструкції, які мають люфти та збільшені зазори між елементами конструкції, що блокуються.

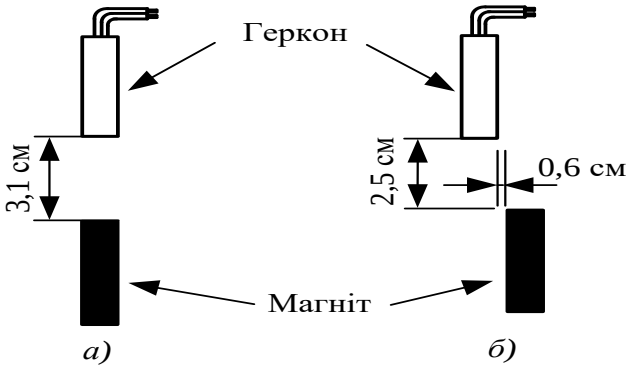

Рис. 8.2 Робочий зазор МКС

Зазор відпускання.

Параметр визначає величину зазору, при якому відбувається розмикання контактів геркона.

За способом монтажу можна виділити дві основні групи МКС: призначені для встановлення на поверхні конструкції (дверях, рамі і т.п.) (рис. 8.3 *а*) і для прихованого встановлення (всередині елементу, що блокується) (рис. 8.3 *б*).

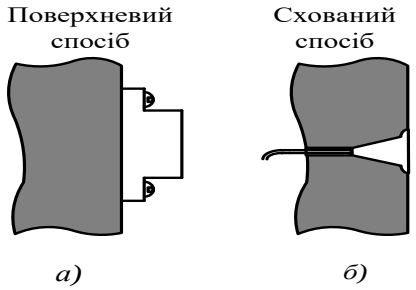

Рис. 8.3 Способи встановлення МКС

Захист від блокування

Один з основних принципів побудови систем безпеки полягає в тому, що система повинна бути стійкою до можливих спроб втручання в неї з метою блокування, виводу її з ладу. Варіант такого способу блокування МКС - впливати

сильним магнітним полем: наприклад, піднести сильний магніт до зовнішньої частини дверей, за якою розташований МКС. Найпростіший і в той же час надійний спосіб протидіяти цьому - заглиблений, схований монтаж. При цьому зловмиснику невідоме місце положення МКС.

З конструктивних засобів можна відзначити екранування датчика від блокування. Це досягається використанням спеціального екрана, що захищає МКС від можливого впливу.

Для контролю цілісності шлейфа, у який включений МКС, використовують додаткове нормально замкнуте коло контролю обриву шлейфа. Так, сповіщувачі серії EMPS компанії С&К мають додаткову пару виводів такого нормально замкнутого кола.

2. Пасивний інфрачервоний сповіщувач

Пасивні інфрачервоні сповіщувачі руху, відомі також за назвою оптико-електронні, є пристроями, які найчастіше використовуються для виявлення руху людини у контрольованій зоні рис. 8.4 [13].

Рис. 8.4 Сучасний пасивний ІЧ сповіщувач SWAN QUAD Crow

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. Тим самим вирішується задача реєстрації вторгнення не тільки через найбільш уразливі місця, але практично при будь-якому шляху проникнення: через вікна, двері, проломи підлоги, стелі, стіни. Очевидно, що це значно ефективніше, ніж блокування тільки периметра об'єкта (вікон, дверей і тому подібних конструктивних елементів об'єкта). Це не виключає блокування першого рубежу охорони, що дозволяє в більшості випадків отримати ранній сигнал тривоги і мати більше часу на відповідну реакцію.

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.

Основні елементи, які повинні входити до складу ПІЧ-сповіщувача для того, щоб він реєстрував зміну ІЧ-випромінювання, показані на (рис. 8.5) [3].

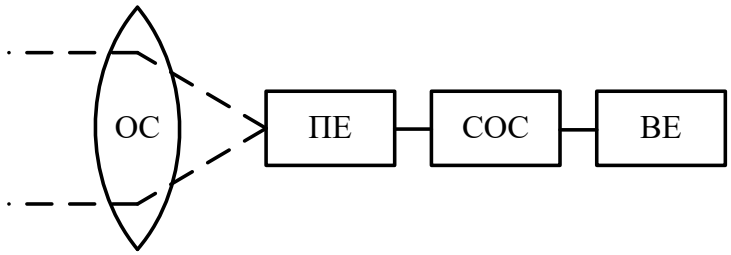

Рис. 8.5 Основні елементи ПІЧ-випромінювання

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'єкт, активізується виконавчий елемент. Зазвичай, останній елемент - це реле з контактами, які вмикаються в шлейф сигналізації.

Конструкція піроприймача.

Чутливий елемент із піроелектричного матеріалу має електроди, що утворюють конденсатор великої ємності (рис. 8.6). Через те, що піроприймач призначений для виявлення дуже малих рівнів випромінюваної інфрачервоної енергії, струм піроелемента досить малий. Тому для перетворення цього струму в прийнятну напругу й узгодження високоомного опору кола піроприймача з

наступними каскадами тракту обробки сигналу використовують високоомний резистор і польовий транзистор з малим струмом витоку.

Піроелектричний матеріал розташовується на спеціальній підкладці, на якій також встановлюються високоомний резистор та польовий транзистор. Піроприймач розміщають у корпусі зі смуговим фільтром. Смуга пропускання фільтра визначається призначенням піроприймача.

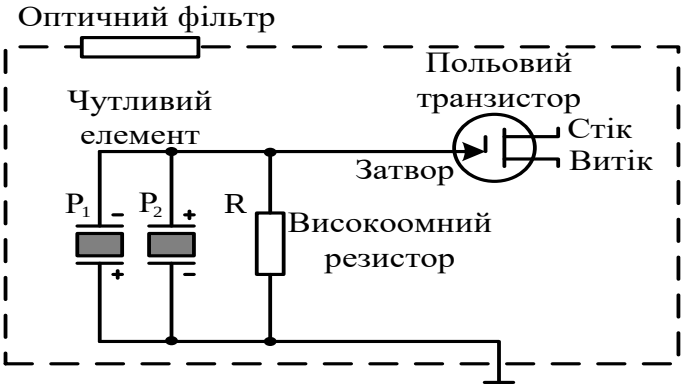

Рис. 8.6 Основні елементи піроприймача

Основні типи діаграм спрямованості ПІЧ сповіщувачів.

Одна з основних характеристик сповіщувача - це зона виявлення, обумовлена діаграмою спрямованості. 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. У межах зони виявлення сповіщувач повинен виявляти рух стандартної цілі, яка переміщується в зоні виявлення поперечно її бічній границі в діапазоні швидкостей 0,3-3 м/с. При цьому відстань між сповіщувачем і ціллю повинна залишатися постійною.

Приклад типової реальної діаграми спрямованості приведений на (рис. 8.7), на (рис. 8.7 а) зображений вид зверху, а на (рис. 8.7 б) - вид збоку. 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.

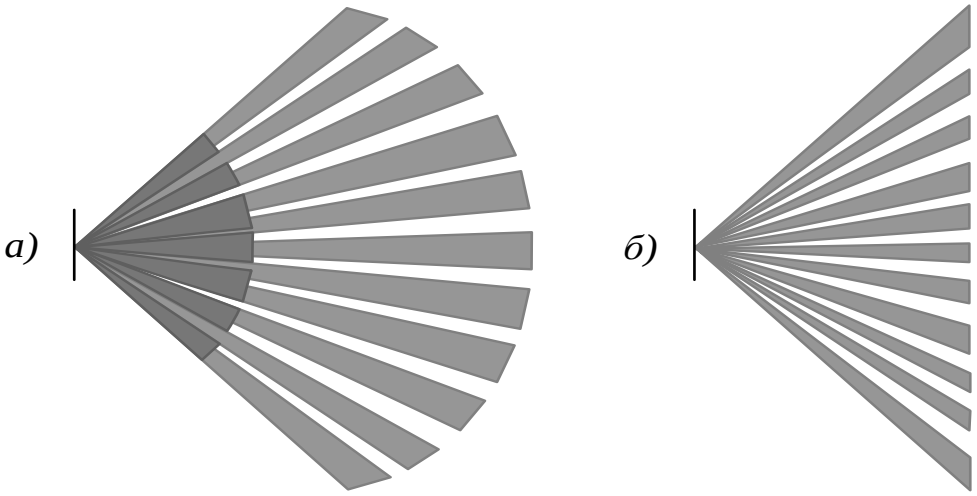

Рис. 8.7 Об'ємна діаграма спрямованості

Нерівномірність чутливості приводить до того, що той самий порушник, рухаючись в різних ділянках зони, буде викликати появу сигналів, що значно відрізняються по амплітуді. При такому самому рівні шумів це означає різне співвідношення сигнал/шум для різних ділянок зони. Пов'язано це насамперед з тим, що коефіцієнт підсилення тракту обробки сигналу повинен вибиратися виходячи з вимоги забезпечення необхідної імовірності правильного виявлення в гірших умовах, у частині діаграми з найменшою чутливістю. Однак при цьому в ділянках з більшою чутливістю зростає не тільки імовірність правильного виявлення, але й імовірність помилкових тривог.

Інший досить 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. 8.8) і «вертикальна» чи «бар'єр вертикальна фіранка» (рис. 8.9).

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. Помітимо одну важливу особливість. При використанні таких діаграм повинна установлюватися висока чутливість сповіщувача.

При збільшенні кута розкриву зростає площа поверхні, в якій сповіщувач сприймає теплове випромінювання, у тому числі і природний шумовий фон. Це приводить до зростання рівня шумів. У той же час сигнал від реальної цілі залишається тим самим. Отже зменшується відношення сигнал/шум і, як наслідок,

погіршуються характеристики виявлення (зменшується імовірність виявлення і зростає імовірність помилкової тривоги).

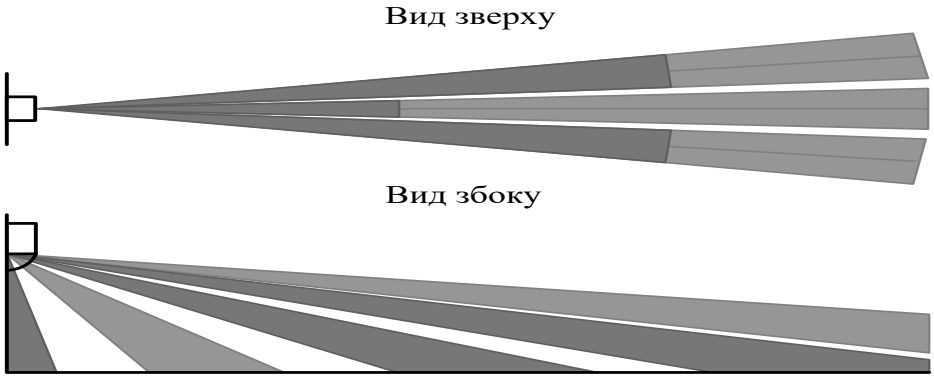

Рис. 8.8 Коридорна діаграма спрямованості

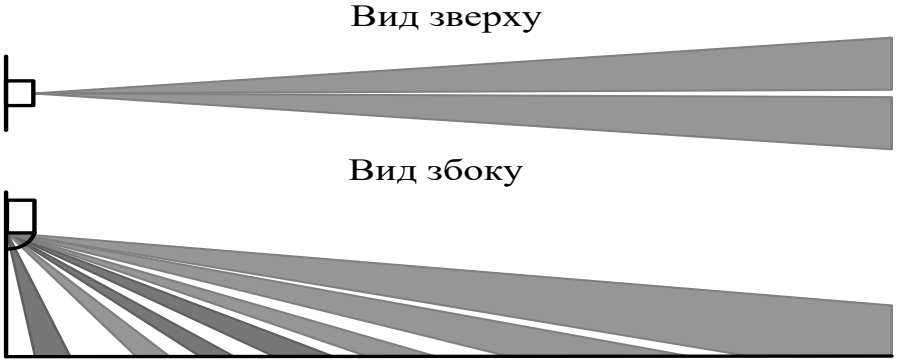

Рис. 8.9 Діаграма спрямованості “вертикальна штора”

Вищевказане підтверджується і тим, що ті самі сповіщувачі при використанні “коридорної” лінзи (з меншим кутом розкриву) мають, як правило, більшу дальність дії, ніж з лінзою типу “широкий кут”. Вибір значення кута менше 90° (за винятком випадків спеціальних вузьких, так званих коридорних діаграм) погіршує можливості перекриття діаграмою спрямованості контрольованого приміщення.

3 Сповіщувачі розбиття скла

Одним з найбільш поширених елементів ОІД є конструкції із скла. Це вікна, скляні двері та інші елементи. З огляду на значну уразливість скляних поверхонь, їхню доступність для руйнування з наступним проникненням формування сигналів тривоги при розбитті скла є однією з важливих задач систем охоронної сигналізації. Основні вимоги до сповіщувачів розбиття скла (як і до будь-яких інших сповіщувачів) - є висока імовірність правильного виявлення $P_{пв}$ розбиття скла при мінімальному рівні імовірності помилкових тривог $P_{пт}$.

Відомо, що 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 визначеного розміру, відбувається механічне руйнування скла. Воно супроводжується акустичними коливаннями високих частот. 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.

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 класичному випадку акустичний сповіщувач складається з мікрофона М, фільтра Ф, що виділяє найбільш типові спектральні складові сигналу, схеми обробки СО і виконавчого елемента - реле Р (рис. 8.10).

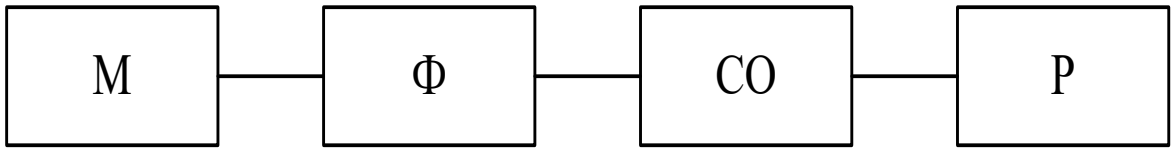

Рис. 8.10 Склад акустичного сповіщувач розбиття скла

Алгоритми роботи акустичних сповіщувачів.

Одноканальний граничний алгоритм.

Структурна схема найпростішого акустичного сповіщувача, що використовує одноканальний пороговий алгоритм, зображена на рис. 8.10. Відповідні часові діаграми його функціонування представлені на рис. 8.11.

Схема обробки такого пристрою містить у собі підсилювач, детектор і пороговий пристрій. У розглянутому сповіщувачі смуга пропускання фільтра повинна бути досить широкою, щоб пропускати всі основні спектральні складові сигналу розбиття скла. З мікрофона можуть надходити сигнали, обумовлені

акустичними коливаннями, викликаними різними причинами. Спектральний склад цих коливань буде істотно відрізнятися.

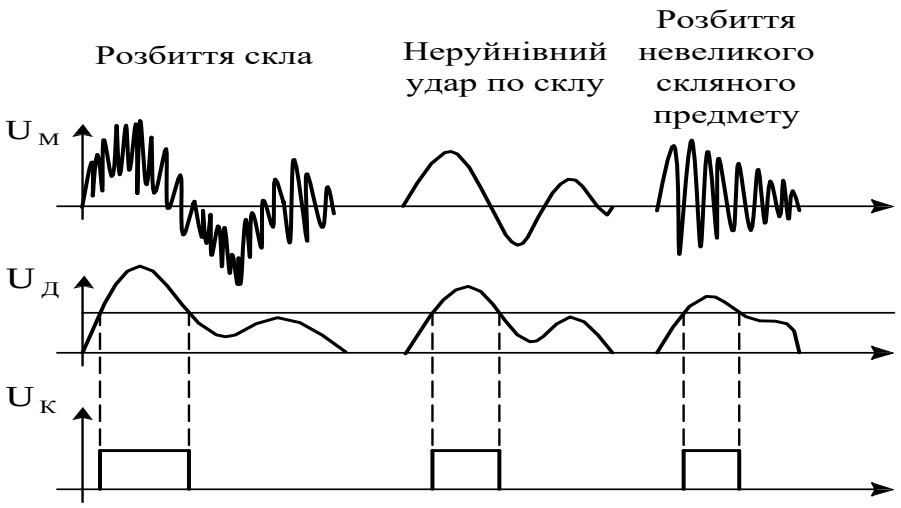

Рис. 8.11 Часові діаграми роботи одноканального акустичного сповіщувача

У першому випадку при реальній події розбиття контрольованого скла на виході сповіщувача виникає сигнал $U_д$ з амплітудою, достатньою для реєстрації тривоги ($U_к$). Однак, реєстрація тривоги (помилкової) може мати місце й в інших випадках, коли присутні тільки сигнали достатньої інтенсивності, у спектрі яких є або тільки низькочастотні, або тільки високочастотні складові. У такий спосіб при деякій привабливості, викликаній простотою і, отже, більш низькою ціною, такі сповіщувачі значно поступаються у функціональних характеристиках. Зокрема, вони в значно більшому ступені піддаються впливу джерел помилкових тривог.

Звуження смуги пропускання фільтра дозволить знизити імовірність помилкових тривог. Але при цьому падає й імовірність правильного виявлення.

Двоканальний граничний алгоритм.

Реєстрація послідовності акустичних коливань, що відповідають деформації скла (низькочастотні коливання) і його руйнуванню (високочастотні), покладена в основу принципу дії більшості сучасних акустичних сповіщувачів розбиття скла. Прийняті роздільно у визначеній часовій послідовності ці сигнали порівнюються по інтенсивності з фіксованими значеннями порогових рівнів для кожного виду коливань. При їхньому перевищенні сповіщувач фіксує тривогу.

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. Такий принцип обробки

використовується, наприклад, у популярних сповіщувачах серії FlexGuard компанії C&K Systems. Важливо відзначити, що наявність яскраво вираженої низькочастотної складової обумовлена насамперед умовою необхідності виявлення розбиття скла, закріпленого в рамі.

На рис. 8.12 зображена структурна схема сповіщувача розбиття скла, що реалізує розглянутий вище алгоритм.

Сповіщувач складається з наступних складових:

- мікрофон (М);
- канал, що реєструє низькочастотні коливання, які відповідають деформації (вигину) скла. Канал складається з фільтра низьких частот (ФНЧ), порогового пристрою (ПП1) і одновібратора (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 збігу "І";
- схему фіксації (СФ), що забезпечує або включення реле на визначений час, або фіксацію реле (пам'ять тривоги);
- виконавчий елемент (реле).

Схема працює в такий спосіб. У вихідному стані канал «звук» закритий, низькочастотний канал відкритий. При виникненні тільки низькочастотних коливань достатньої інтенсивності сигнал на виході ФНЧ перевищує пороговий рівень. Запускається одновібратор. Сигнал з виходу одновібратора надходить на схему “І”. Однак, якщо відсутній вихідний сигнал каналу обробки високочастотних коливань, то схема “І” закрита і реле не спрацьовує.

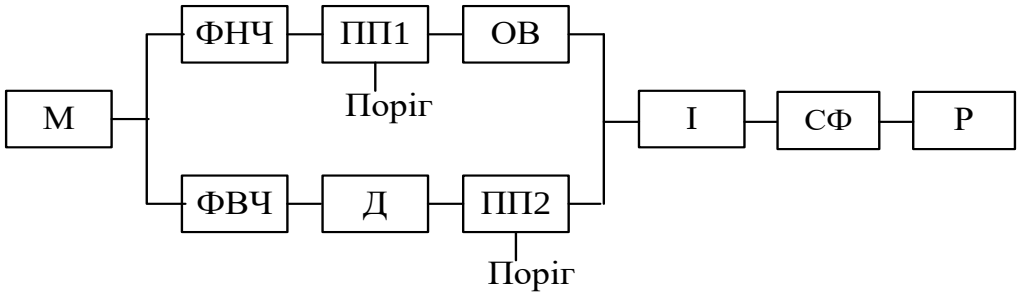

Рис. 8.12 Структурна схема двоканального сповіщувача розбиття скла

Якщо виникають тільки високочастотні коливання достатньої інтенсивності, то на виході фільтра високих частот з'явиться високочастотний сигнал. Амплітудний детектор виділяє огинаючу цього сигналу, але пороговий пристрій закритий сигналом одновібратора і схема “І” не спрацьовує.

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.

Контрольні запитання

1. Для чого призначений магнітоконтактний сповіщувач.
2. Як конструктивно влаштований МКС?
3. Назвати основні параметри МКС
4. Від чого залежать робочий зазор та зазор відпускання МКС?
5. Як захистити МКС від блокування
6. Яке призначення сповіщувачів розбиття скла?
7. Який фізичний принцип дії використовується у сучасних сповіщувачах розбиття скла?
8. Охарактеризувати складові процесу розбиття скла, та їх характеристики.
9. Розповісти склад сповіщувача розбиття скла, що реалізує одноканальний граничний алгоритм.
10. Розповісти склад сповіщувача розбиття скла, що реалізує двоканальний граничний алгоритм.
11. За рахунок чого завадостійкість сповіщувача двоканального граничного алгоритму вища ніж у сповіщувача одноканального граничного алгоритму?
12. Що являється чутливим елементом сповіщувача розбиття скла?
13. Дати визначення пасивного ІЧ сповіщувача та для чого він призначений.
14. Принцип дії пасивного ІЧ сповіщувача та його склад.
15. Визначення зони виявлення пасивного ІЧ сповіщувача, чим вона визначається, на що впливає.
16. Охарактеризувати коридорну та вертикальна штора діаграми спрямованості пасивного ІЧ сповіщувача
17. Охарактеризувати об'ємну діаграму спрямованості пасивного ІЧ сповіщувача
18. Яка залежність між кутовим розміром пелюстків діаграми спрямованості та їхньою кількістю та як це впливає на надійність виявлення порушника?

Лекція № 9

Тема. Технології виявлення перетину порушником інформаційної безпеки межі контрольованої зони ОІД

ПЛАН ЛЕКЦІЇ

1. Активний інфрачервоний сповіщувач
2. Радіопроменеві охоронні системи
3. Радіохвильові охоронні системи на ефекті хвилі, що витікає

Активний інфрачервоний сповіщувач

За принципом роботи і структурою ІЧЗВ розділяють на **активні** (двопозиційні) і **пасивні**. Активні ІЧЗВ (рис. 9.1) частіше застосовують для охорони протяжних рубежів і периметрів. Для охорони приміщень і окремих предметів перевага віддається пасивним ІЧЗВ.

Рис. 9.1 Активна ІЧ охоронна система

Принцип дії активного інфрачервоного (ІЧ) сповіщувача (далі активного ІЧС) полягає в створенні променевого бар'єра, при перериванні якого активний ІЧС виробляє сигнал тривоги. Розрізняються кількістю ІЧ променів (1 , 2, 3) [3].

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 чекання сигнал від передавача зникає (на прямій між передавачем і приймачем з'явився об'єкт, що екранує сигнал), то активний ІЧС виробляє сигнал тривоги.

Для збільшення дальності дії приладу в передавачі і приймачі формується однопелюсткова діаграма спрямованості, як показано на рис. 9.2.

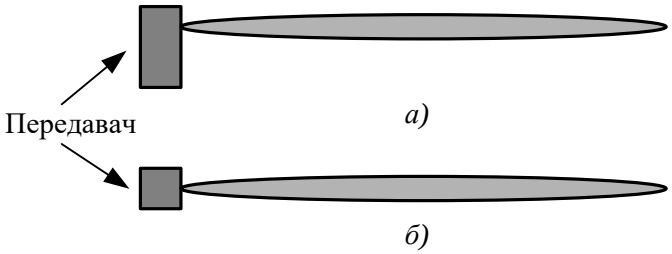

Рис. 9.2 Діаграма спрямованості ІЧ-приймача та передавача у вертикальній (а) і горизонтальній (б) площинах

Принцип дії активних ІЧЗВ можна пояснити, скориставшись узагальненою структурною схемою (рис. 9.3).

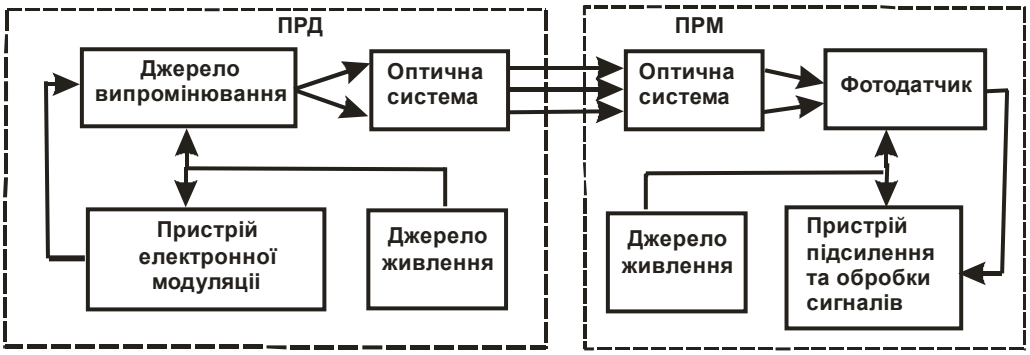

Рис. 9.3 Узагальнена структурна схема активних ІЧЗВ

Випромінюючим елементом є інфрачервоний світлодіод.

Вихідний сигнал джерела випромінювання модулюється сигналом низької частоти, некратної частоті 100 Гц, що виробляється генератором. Модуляція необхідна для підвищення завадостійкості і вірогідності спрацювання активного ІЧС. Оптична система активного ІЧС призначена для формування діаграми спрямованості з заданими параметрами. Приймачем активного ІЧС є фотоелемент, чутливий до інфрачервоного випромінювання.

Оптична система джерела випромінювання (скорочено передавача - ПРД) створює вузьконаправлений промінь ІЧ-випромінювання. Як джерело ІЧ-випромінювання використовують напівпровідникові випромінюючі діоди з робочою довжиною хвилі 0,94 мкм, які розташовують у фокусі оптичної системи.

Для забезпечення необхідного значення струму через діод і зниження струму споживання ПРД живлення діода здійснюється імпульсною

промодульованою напругою, яка виробляється в пристрої електронної модуляції. Кут розбіжності проміня як правило, складає 1,5°...2°, що дозволяє отримати необхідну потужність випромінювання ПРД для блокування рубежу протяжністю 200…250 м з урахуванням дії метеорологічних чинників (туман, дощ, снігопад).

Промінь (потік ІЧ-випромінювання) ПРД направлений на оптичну систему ПРМ, кут поля зору якого складає зазвичай 2°… 3°. Невеликий кут поля зору ПРМ дозволяє зменшити вплив побічних фонових засвічень фотоприймача. Проте в ПРМ потрапляє потік ІЧ-випромінювання, що охоплюється тільки світловим діаметром $D_{СВ}$ оптичної системи. Тому чутлива зона активного двохпозиційного ІЧЗВ є променем діаметром постійного перетину по всій довжині ділянки, що блокується. 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.

Залежно від кількості променів і їх розташування (горизонтальне або вертикальне) ІЧЗВ можуть виконувати різні тактичні завдання. Горизонтальне розташування двох променів дозволяє за рахунок тимчасової обробки сигналів визначати напрям руху порушника. Вертикальне розташування променів в активних ІЧЗВ підвищує надійність блокування рубежів і периметрів в порівнянні з однопроменевими ЗВ.

Приймач і передавач розміщені в однакових корпусах, мають подібну внутрішню компоновку і відрізняються лише схемними рішеннями (рис. 9 4).

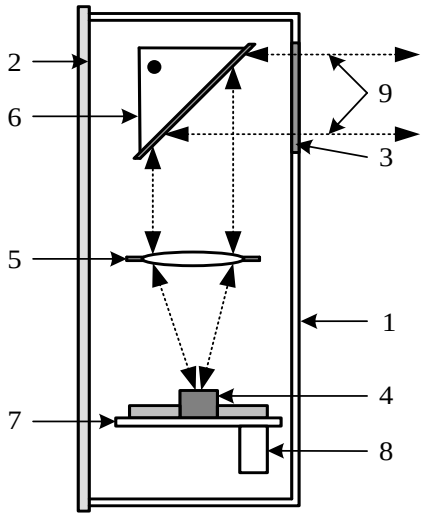

Рис. 9.4 Розміщення елементів активного ІЧС всередині корпусу (1 – передня кришка корпусу, 2 – задня кришка корпусу, 3 – ІЧ-прозоре вікно, 4 – ІЧ-чутливий (випромінюючий для передавача) елемент, 5 – фокусуюча система, 6 – дзеркало, 7 – клемна колодка для підключення живлення та сигнальних проводів, 8 – напрям ходу променів)

Одним з чинників, обмежуючим можливість використання ІЧЗВ, є туман з метеорологічною дальністю видимості менше 200.. .250 м, при якому відбувається видача помилкових сигналів тривоги або втрата працездатності. Крім того, у весняно-осінній і зимовий періоди року активні ІЧЗВ вимагають обігріву оптичних систем, що також обмежує їх застосування при невеликих ємностях джерел постійного струму.

Перешкоди в пасивних ІЧЗВ. Перейдемо до аналізу дії завад, що викликають помилкове спрацьовування пасивних ІЧЗВ. Під завадою розумітимемо будь-яку дію зовнішнього середовища або внутрішні шуми приймального пристрою, не пов'язані з рухом людини в зоні чутливості ЗВ.

Існує наступна класифікація завад:

- теплові, обумовлені нагріванням фону при дії на нього сонячного випромінювання, конвекційних потоків повітря від роботи радіаторів, кондиціонерів, протягів;

- електричні, такі, що викликаються наведеннями від джерел електро- і радіовипромінювань на окремі елементи електронної частини ЗВ;

- власні, обумовлені шумами піроприймача і тракту посилення сигналу;

- сторонні, пов'язані з переміщенням в зоні чутливості ЗВ дрібних тварин (собаки, кішки, птахи) або комах по поверхні вхідного оптичного вікна ЗВ.

Найбільш значною і небезпечною завадою є теплова, така, що викликається зміною температури ділянок фону, на які направлені променеві зони чутливості. Дія сонячного випромінювання приводить до локального підвищення температури окремих ділянок стіни або підлоги приміщення. При цьому поступова зміна температури не проходить через схеми фільтрації приладу, проте, порівняно різкі і “несподівані” її коливання, зв'язані, наприклад, із затінюванням сонця хмарами, що проходять, або проїздом транспорту, викликають перешкоду, аналогічну сигналу від проходження людини. Амплітуда завади залежить від інерційності фону, на який направлений промінь. Наприклад, час зміни температури голої бетонної стіни набагато більший, ніж дерев'яної або обклеєної шпалерами.

При цьому зміна температури при сонячних завадах досягає 1,0...1,5°С, особливо в тих випадках, коли промінь направлений на малоінерційний фон, наприклад на дерев'яну стіну або штору з тканини. тривалість таких перешкод залежить від швидкості затінення і може потрапити в діапазон швидкостей, характерних для руху людини. Необхідно відзначити одну істотну обставину, яка дозволяє боротися з такими завадами. Якщо два промені направлені на сусідні ділянки фону (при відстані між ними 0,5... 1,0 м), то вигляд і амплітуда завадового сигналу від дії сонця практично однакові в кожному промені, тобто у наявності

сильна кореляція завад. Це дозволяє відповідною побудовою схеми подавити їх за рахунок віднімання сигналів,

Конвективні завади обумовлені дією потоків повітря, що переміщаються, наприклад протягів при відкритій кватирці, щілин у вікні, а також побутових опалювальних приладів – радіаторів і кондиціонерів. Потоки повітря викликають хаотичну флуктуаційну зміну температури фону, амплітуда і частотний діапазон якого залежать від швидкості потоку повітря і характеристик фонової поверхні. На відміну від сонячного засвічення конвективні перешкоди від різних ділянок фону, що діють навіть на відстані 0,2.. .0,3 м, слабо корельованні між собою і їх віднімання не дає ефекту.

Електричні завади виникають при включенні будь-яких джерел електро- і радіовипромінювання, вимірювальної і побутової апаратури, освітлення, електродвигунів, радіопередавальних пристроїв, а також при коливаннях струму в кабельній мережі і лініях електропередач. Значний рівень перешкод створюють також розряди блискавок.

Чутливість піроприймача дуже висока – при зміні температури на 1°С вихідний сигнал безпосередньо з кристала складає долі мікровольта, тому наведення від джерел завад в декілька вольт на метр можуть викликати завадовий імпульс, в тисячі разів більший за корисний сигнал. Проте велика частина електричних завад має малу тривалість або крутий фронт, що дозволяє відрізнити їх від корисного сигналу.

Власні шуми піроприймача визначають найвищу межу чутливості ІЧЗВ і мають вигляд білого шуму. У зв'язку з цим методи фільтрації тут не можуть бути використані. Інтенсивність завади збільшується при підвищенні температури кристала приблизно в два рази на кожні десять градусів. Сучасні піроприймачі мають рівень власних шумів, що відповідвють зміні температури на 0,05…0,15°С.

Методи підвищення завадостійкості пасивних ІЧЗВ.

Диференціальний метод прийому ІЧ-випромінювання набув досить широкого поширення. Суть цього методу полягає в наступному: за допомогою приймача з двох площадок формуються дві просторово рознесені зони чутливості. Сигнали, що формуються в обох каналах, взаємно віднімаються:

$$U_{вих}(t) = U1(t) - U2(t)$$

Зрозуміло, що дві просторово рознесені зони чутливості не можуть бути перетнуті рухомим об'єктом одночасно. Сигнали в каналах в цьому випадку виникають по черзі, отже, амплітуда їх не зменшується. З формули (1) виходить, що перешкода на виході диференціального приймача дорівнює нулю при сумісному виконанні наступних умов:

1. Форми перешкод в каналах збігаються.

2. Амплітуди перешкод однакові.

3. Перешкоди мають однакове тимчасове положення.

У разі сонячної перешкоди виконуються умови 1 і 3 (з точністю до рівня флуктуаційного шуму). Умова 2 виконується тільки у разі, коли як фон в обох каналах служить один і той же матеріал або кути падіння сонячної енергії на фон однакові в обох каналах, або в обох каналах потік сонячного випромінювання потрапляє на всю площу фону, що обмежує зони чутливості.

Оптимальна частотна фільтрація. Ефективне придушення перешкод цим методом можливо при істотній відмінності в частотних спектрах сигналів і перешкод. З приведених вище даних виходить, що такої відмінності в нашому випадку немає. Тому використання цього методу для повного придушення перешкод не є можливим. Основним видом шуму, що визначає чутливість ІЧЗВ, є власний шум приймача. Тому оптимізація смуги пропускання підсилювача залежно від спектру сигналу і характеру шуму приймача дозволяє реалізувати граничні можливості приймальної системи.

Оптична спектральна фільтрація. Суть методу оптичної спектральної фільтрації така ж, як і у разі оптимальної частотної фільтрації. При спектральній фільтрації перешкода пригнічується за рахунок відмінностей в оптичних спектрах сигналів і перешкод. Ці відмінності практично відсутні (без урахування тонкої структури спектрів) для конвективної перешкоди і для складової сонячної перешкоди, що виникає за рахунок зміни температури фону під дією сонячного випромінювання, проте спектр відбитої від фону складової сонячної перешкоди, значною мірою відрізняється від спектру сигналу. Спектральна щільність енергетичної світимості абсолютно чорного тіла визначається формулою Планка:

$$\mathrm{M}(\lambda, \mathrm{T}) = 2\pi c^2 h \lambda^{-5} \left(e^{ch/k\lambda \mathrm{T}} - 1\right)^{-1},$$

де:

λ – довжина хвиль;

k – постійна Больцмана (k = 1,3805 · 10^{-23} Дж/град) ;

T – температура тіла;

h – постійна Планка;

c – швидкість розповсюдження випромінювання в вакуумі.

Оптимальна просторово-частотна фільтрація. Відомо, що характеристики виявлення в умовах оптимальної лінійної фільтрації однозначно пов'язані з величиною відношення сигнал/завада.

По фізичному змісту величина відношення сигнал/завада є відношенням енергії сигналу до спектральної щільності потужності перешкоди. Очевидно, що при зміні тілесного кута елементарної зони чутливості міняється інтенсивність перешкоди, що випромінюється фоном і потрапляє в приймальний канал. В той же час амплітуда сигналу залежить від геометричної форми (конфігурації) елементарної зони чутливості. В результаті проведених досліджень на предмет визначення при якій конфігурації елементарної зони чутливості величина **μ** досягає максимального значення було встановлено.

Для випадку флуктуаційної фонової перешкоди максимальне значення відношення сигнал/фонова перешкода досягається при збігу геометричної форми елементарної зони чутливості з формою об'єкту. Цей висновок застосують і для випадку імпульсної сонячної перешкоди. Підтвердженням тому є очевидний факт, що при збільшенні тілесного кута зони чутливості від значення, рівного тілесному куту, під яким видно об'єкт, амплітуда сигналу не змінюється, а амплітуда сонячної перешкоди росте пропорційно тілесному куту зони чутливості. Тобто метод оптимальної просторово-частотної фільтрації дозволяє підвищити перешкодостійкість пасивного оптичного засобу виявлення як до конвективної, так і до сонячної перешкод.

Дводіапазонний метод прийому ІЧ випромінювань. Суть цього методу полягає у введенні в ІЧЗВ другого каналу, що забезпечує прийом ІЧ випромінювань у видимому або ближньому ІЧ діапазонах, з метою отримання додаткової інформації, що відрізняє сигнал від перешкоди. Використання такого каналу в сукупності з основним (тепловим) каналом в умовах одного приміщення малоефективне, оскільки як сигнал, так і перешкода за наявності освітленості, формуються в обох спектральних діапазонах (видимому і тепловому). Значно ефективнішим є використання каналу видимого діапазону при його установці поза приміщеннями, що охороняються, в місцях, недоступних для блокування цього каналу штучними джерелами світла. В цьому випадку при зміні сонячної освітленості канал формує сигнал, що забороняє можливе спрацьовування ІЧЗВ під впливом сонячної перешкоди. При такій організації дводіапазонний метод дозволяє повністю ліквідовувати помилкові спрацьовування ІЧЗВ, які можливі за рахунок виникнення сонячних перешкод. Можливість блокування теплового каналу на час дії перешкоди очевидна.

Параметричні методи підвищення завадостійкості ІЧЗВ. У основу параметричних методів підвищення завадостійкості ІЧЗВ покладена ідентифікація корисних сигналів по одиному або сукупності параметрів характерних для об'єктів, що викликають появу цих сигналів. В якості параметрів, можуть бути використані швидкість руху об'єкту, його габарити, відстань до об'єкту. На практиці, як правило, конкретні значення параметрів заздалегідь не відомі. Проте

є деяка область їх визначення. Так, швидкість людини, що пересувається пішки, менше 7 *м/с.* Сукупність таких обмежень може істотно звузити область визначення корисного сигналу і, отже, зменшити вірогідність помилкового спрацьовування. Основною умовою реалізації цього методу є широка смуга пропускання приймального тракту, необхідна для прийому сигналу без спотворення його форми, тобто в цьому випадку виключається застосування методу оптимальної фільтрації. Неспотвореним в процесі оптимальної фільтрації параметром є тривалість затримки між сигналами, що виникає в просторово-рознесених каналах. Тому ідентифікація по цьому параметру може проводитися без розширення смуги пропускання приймального тракту.

Використання незалежних каналів дозволяє підвищити стійкість приладу і до конвективних перешкод, оскільки кінцеве рішення про виявлення ухвалюється тільки у разі виявлення сигналів хоч би в двох каналах протягом деякого тимчасового інтервалу, що визначається максимально можливою затримкою сигнального імпульсу між каналами. При цьому вірогідність помилкової тривоги визначається виразом, $P_{ПТ} = P_{ПТ1} \cdot P_{ПТ2}$, де, $P_{ПТ1}$ $P_{ПТ2}$, – вірогідність помилкової тривоги в окремих каналах.

Таблиця № 9.1. Методи підвищення перешкодостійкості ІЧЗВ

Метод	**Позитивні якості**	**Негативні якості**
Диференціальний	Часткове придушення сонячних та конвективних перешкод	Низька перешкодостійкість до некорельованих перешкод
Частотна фільтрація	Частотне придушення сонячних та конвективних перешкод	Складність реалізації для багатоканальних систем
Дводіапазонний	Повне придушення сонячних перешкод. Простота тракту обробки	Можливість блокування засобу зовнішними джерелами світла. Не придушуються конвективні перешкоди. Необхідність додаткового оптичного каналу.
Оптимальна просторово-частотна фільтрація	Часткове придушення фонових та сонячних перешкод. Простота реалізації.	Необхідність використання приймачів із спеціальною формою чутливої площадки
Параметричні методи	Часткове придушення фонових перешкод. Значне придушення сонячних перешкод.	Складність тракту обробки

Порівняльний аналіз методів підвищення завадостійкості ІЧЗВ. Розглянуті вище методи підвищення перешкодостійкості ІЧЗВ досить різноманітні як по своїй фізичній суті, так і по складності реалізації. Для

зручності порівняння цих методів по сукупності позитивних і негативних якостей розроюлено таблицю 9.1.

З таблиці видно, що жоден метод окремо не дозволяє повністю подавити всі перешкоди. Проте, одночасне використання декількох методів дозволяє істотно підвищити завадостійкість ІЧЗВ при незначному ускладненні приладу в цілому. По сукупності позитивних і негативних якостей найбільш переважним є поєднання: спектральна фільтрація + просторово-частотна фільтрація + параметричний метод.

Радіопроменеві охоронні системи

Двопозиційні радіопроменеві системи (охорона периметра ОІД) (рис. 9.5) [14].

Принцип дії.

Інженерні засоби охорони периметра різноманітні та відрізняються один від одного не лише технічно-експлуатаційними характеристиками, а й призначенням. Ефективними технічними елементами вважатимуться радіопроменеві засоби виявлення.

Принцип дії таких систем є простим. Радіопроменева система складається з передавача та приймача, які утворюють невидиму зону виявлення, «позначаючи» межі (рис. 9.5). У подальшому система здійснює контроль електромагнітного поля між приймачем і передавачем. Поле має витягнуту еліптичну форму. При перетині людиною зони виявлення, параметри поля змінюються і приймач фіксує зміну амплітуди сигналу. Якщо значення амплітуди вийшло за норму, датчик «видає сигнал тривоги». Розміри зони виявлення можуть бути різними: перш за все, вона залежить від того, наскільки далеко один від одного знаходяться приймач і передавач. Важливо відзначити, що така система демонструє свою високу ефективність лише на певних територіях: ландшафт має бути рівним, без чагарників, дерев тощо.

Особливості радіопроменевих засобів виявлення.

Радіопроменеві засоби виявлення мають недолік, який виявляється у виникненні «мертвих зон». У безпосередній близькості від передавача та приймача чутливість системи дещо знижена, що може позначитися на ефективності охорони. Тим не менш, цей недолік легко нівелювати - достатньо зробити установку з перекриттям кілька метрів. Важливо враховувати і той факт, що радіопроменеве засіб виявлення призначене для запобігання проникненню порушників, які пересуваються стоячи або зігнувшись. Тому проектуючи комплексну охоронну систему, цю особливість необхідно усунути шляхом встановлення інших елементів охорони.

Радіопроменевий засіб має досить широку зону чутливості. Це, своєю чергою, обмежує спектр застосування. Наприклад, не рекомендується встановлювати таку систему на об'єктах, де до зони охорони можуть випадково потрапити інші суб'єкти: транспорт, люди. Якщо об'єкт потребує встановлення саме радіопроменевої системи, підвищення її ефективності рекомендується облаштувати зону відчуження (розмістити додаткове огородження).

Встановлення блоків радіопроменевих систем повинно здійснюватися на стінах споруд, на огорожі або на ґрунті. Безпосередньо перед встановленням системи необхідно підготувати територію - прибрати ландшафтні елементи та видалити рослинність.

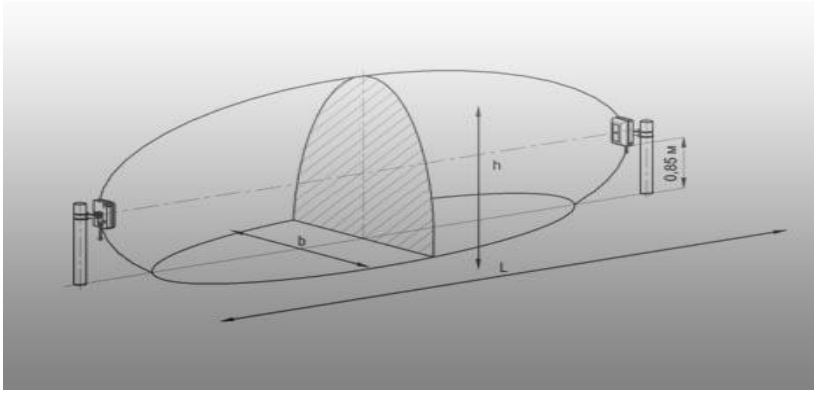

Рис. 9.5 Двопозиційна радіопроменева система

Радіохвильові охоронні системи на ефекті хвилі, що витікає (рис. 9.6, рис. 9.7) [15].

Термін “лінія витікаючої хвилі” (ЛВХ) пов'язаний з особливостями конструкції чутливого елемента (ЧЕ). ЧЕ являє собою екранований перфорований кабель, в якому зовнішній провідник не забезпечує повного екранування центрального провідника, певна частина енергії високочастотного сигналу, що передається, випромінюється через отвори у зовнішнє середовище, частина енергії проникає в приймальний кабель такої ж конструкції. У передавальному кабелі встановлюється режим, близький до режиму хвилі, що біжить, а в приймальному кабелі наводиться опорний сигнал.

Принцип дії ЛВХ ґрунтується на реєстрації збурення електромагнітного поля при перетині порушником об'ємної зони виявлення. Відбита від порушника електромагнітна хвиля приймається приймальним кабелем, унаслідок чого відбувається низькочастотна модуляція амплітуди та фази опорного сигналу.

Кабелі (ЧЕ) можуть встановлюватися на огорожу та закопуватись у ґрунт.

Ширина зони виявлення залежить від чутливості кабелю (виду його конструкції), частоти сигналу, відстані між кабелями, параметрів поверхні, що підстилає, способу обробки сигналу. Висота зони виявлення може досягати 1,5м

Перевагами таких систем є:

- при розміщенні кабелів на огорожі - можливість контролю проникнення через «жорсткі» огорожі без додаткового обладнання їх металевими козирками та контроль руйнування «жорстких» конструкцій (залізобетон, цегла, камінь, дерево);

- при встановленні кабелів у ґрунт - можливість створення невидимих надійних рубежів охорони;

- стійкість до впливу рослинності та нечутливість до дрібних тварин та птахів. У сповіщувачі використовується діапазон робочих частот у межах від 40 до 80 МГц, який дозволяє виявити людину та пропустити дрібних та середніх тварин;

- завадостійкість до електромагнітних перешкод;

- стійкість до акустичних та сейсмічних перешкод.

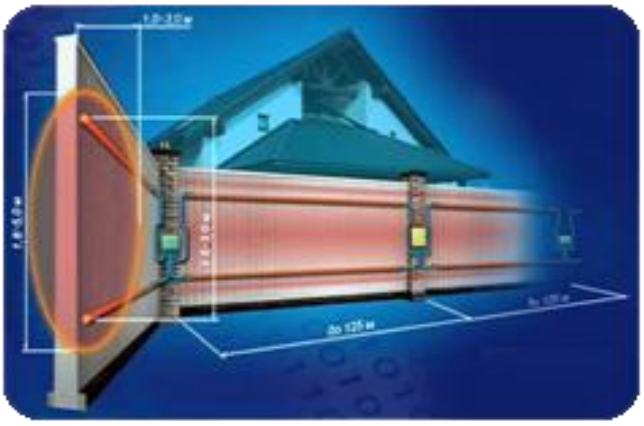

Рис. 9.6 Охорона периметру ОІД ТСО на ефекті хвилі що витікає

Недоліки:

1 Великі масогабаритні характеристики

2 Необхідність захисту оболонки.

3. Наявність демаскуючої ознаки у вигляді електромагнітного випромінювання.

Будь-яке пошкодження діелектричної оболонки може призвести до виходу з ладу дорогого кабелю. Тому найкращим способом є укладання і закладання кабелю в канали, виконані в стіні, що різко збільшує вартість монтажних робіт.

4. Нерівномірність чутливості за довжиною кабелю.

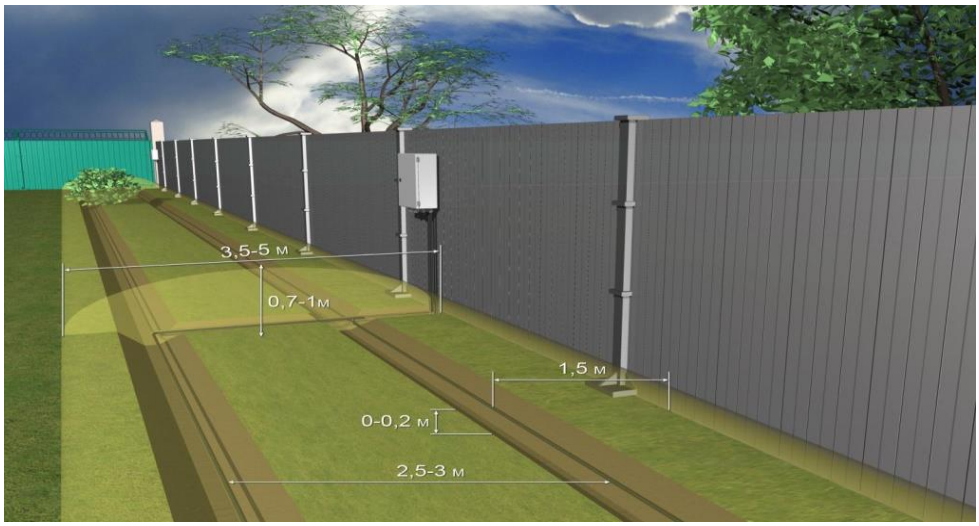

Рис. 9.7 Охорона периметру ОІД системою на ефекті хвилі що витікає

Контрольні запитання

1. Розповісти призначення та принцип дії радіопроменевої охоронної системи.
2. Розповісти призначення та принцип дії радіохвильової охоронної системи.
3. Що використовується у якості чутливого елементу радіохвильової охоронної системи?
4. Назвати переваги технічних систем охорони на ефекті хвилі що витікає.
5. Назвати недоліки технічних систем охорони на ефекті хвилі що витікає.
6. Яке основне обмеження використання радіопроменевої охоронної системи на для охорони периметра?
7. Призначення активної ІЧ охоронної системи
8. Назвати обмеження на використання ІЧ систем
9. Які існують методи підвищення перешкодостійкості ІЧ систем?

3 СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Технічний захист інформації. / Богуш В.М., Бровко В.Д., Козюра В.Д., Кобус О.С. - К: Ліра-К, 2023. - 508 с.
2. Богуш В.М., Бровко В. Д., Кобус О.С., Козюра В.Д. Технічний захист інформації в інформаційних системах. К., Ліра - К, 2022 р., 484 с.
3. Конспект лекцій для студентів з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації» з дисципліни «Програмно-апаратні засоби захисту»/ Уклад. А.М. Котенко, Ю.І. Хлапонін, В.М. Трофимчук -К.:КНУБА, 2025. - 154 с.
4. https://spion-market.com.ua/store/napravlennye-mikrofony-parabolicheskie-lazernye/napravlennyy-mikrofon-akkusticheskoe-ruzhe.html
5. https://eurozakup.com.ua/product-podslushivanie-cherez-stenu-seysmicheskiy-stetoskop-12701311433.html
6. https://spion-market.com.ua/store/napravlennye-mikrofony-parabolicheskie-lazernye/lazernyy-mikrofon-optimic-3000.html
7. https://shpion.com.ua/catalog/zhuchki-i-proslushka/proslushka-zhuchok-gsm-gf19-zvuk-hd-kachestva-30-kv-metrov
8. https://www.ortungsgerate.de/ru/16-proslushivayushcheye-oborudovaniye-2/35-wlan-proslushivayushcheye-oborudovaniye/pro-seriya-wlan-zhuchok-proslushivanie-v-realnom-vremeni-zagruzka-zapisey/
9. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. ДУТ, 2020 – 326 с.
10. https://ela.kpi.ua/items/5e6dc08a-4a31-490a-bee6-81677426f0b4
11. https://xn--80adgebslrpy8u.com.ua/henerator-akustychnoho-shumu-statsionarnyi-rias2hs/
12. https://www.trafo.top/filters.php
13. https://triniti-sb.com.ua/ru/product/spovishchuvach-swan-quad-crow/
14. https://caiman.ua/products/perimeter/radio-beam
15. https://guard-lviv.com.ua/radiokhvylova-okhorona-perymetra