МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

ОПОРНИЙ КОНСПЕКТ ЛЕКЦІЙ

з дисципліни

"ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ"

для студентів освітньо-кваліфікаційного рівня «бакалавр»
спеціальність «Кібербезпека»

Тернопіль
ЗУНУ
2023

Опорний конспект лекцій з дисципліни «Технічні засоби захисту інформації» для студентів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека» / Укл.: Яцків В.В., Кулина С.В. – Тернопіль 2023. – 88 с.

Опорний конспект лекцій складається з частин, що рекомендовані програмою на основі галузевого стандарту вищої освіти України з спеціальності «Кібербезпека та захист інформації».

Укладачі: **Василь ЯЦКІВ**
Сергій КУЛИНА

Рецензенти:
Манжула В.І., к.т.н., доцент, доцент кафедри комп'ютерних наук Західноукраїнський національний університет;
Козак Р.О, к.т.н., доцент, доцент кафедри кібербезпеки Тернопільського національного технічного університету ім. І.Пулюя.

Розглянуто та схвалено на засіданні кафедри кібербезпеки, протокол №10 від 11.04.2023

Розглянуто та схвалено групою забезпечення спеціальності кібербезпека, протокол №4 від 11.04.2023

ЗМІСТ

1. ВИДИ, ДЖЕРЕЛА ТА НОСІЇ ІНФОРМАЦІЇ, ЩО ПІДЛЯГАЮТЬ ЗАХИСТУ

1.1 Властивості інформації як об’єкта захисту.

1.2 Поняття цінності та ціни інформації.

1.3 Складові ціни інформації.

1.4 Види, джерела та носії інформації, що підлягає захисту.

1.5 Класифікація демаскуючих ознак об’єктів захисту.

1.1 Властивості інформації як об’єкта захисту

Поняття інформації Закон України “Про інформацію” визначає інформацію, як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі. Крім того існує ще понад 400 визначень цього терміну.

Згідно з вимогами стандарту України „Про інформацію”, „Про захист інформації в автоматизованих системах” та згідно з Положенням про захист інформації в Україні, затвердженого постановою Кабінету Міністрів України від 9.09.94 р. № 632: ДСТУ 3396.2-97, інформація це відомості про суб’єкти, об’єкти, явища та процеси.

В свою чергу інформація поділяється на (рис. 1.1):

- **інформацію з обмеженим доступом** – інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами;
- **конфіденційну інформацію** – інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними;
- **таємну інформацію** – інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю.

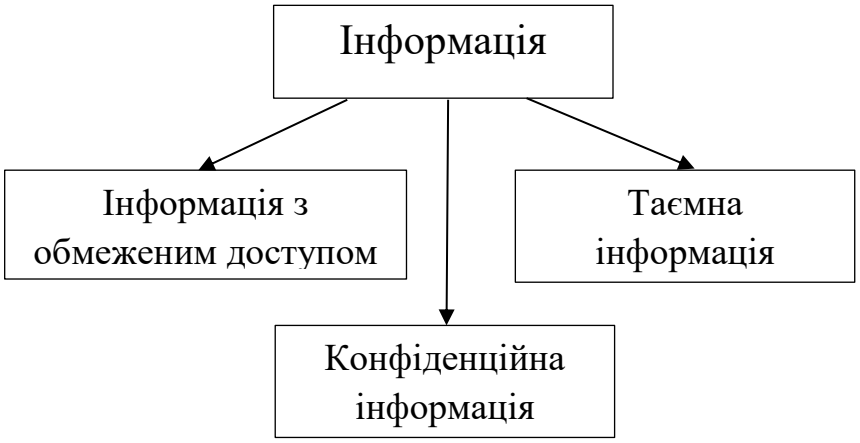

Рисунок 1.1 – Класифікація інформації

Коли ми згадуємо таємницю, то необхідно сказати, що у конкретному випадку мають на увазі військову, державну або комерційну таємницю (рис.1.2).

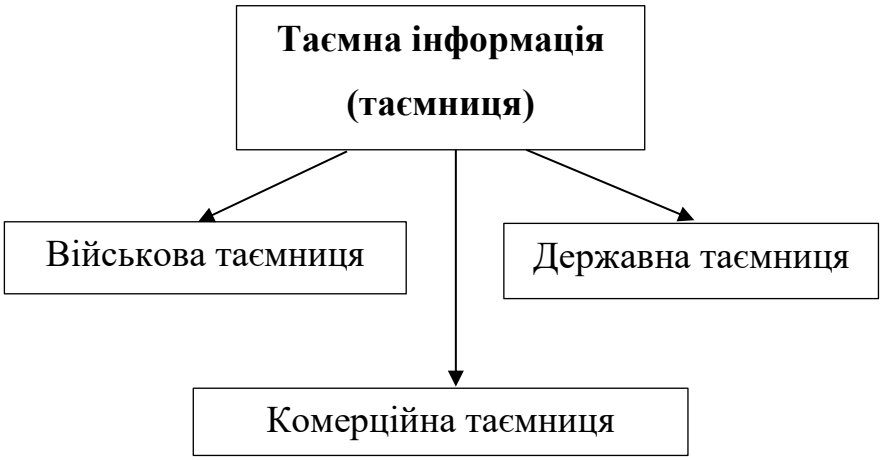

Рисунок 1.2 - Класифікація таємниці

Військова таємниця – це вид таємної інформації, який охоплює відомості у сфері оборони, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди інтересам державної безпеки, бойовій готовності Збройних сил України та інших військових формувань, їх окремих підрозділів, якщо ці відомості не належать до державної таємниці згідно із законодавством України.

Державна таємниця (далі також – секретна інформація) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані в порядку, встановленому Законом України "Про державну таємницю", державною 8 таємницею і підлягають охороні державою.

Комерційна таємниця - це інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

У випадку коли до таємниць отримано не санкціонований доступ, то «кажуть» що стався **витік інформації**. Коли частину інформації або всю було втрачено чи спотворено, то вважається що сталося **порушення цілісності інформації.**

1.2 Поняття цінності та ціни інформації

Корисність інформації завжди конкретна, немає завжди цінної інформації. Інформація корисна або шкідлива для конкретного її користувача а під користувачами звичайно розуміють як одну людину (процес), так і групу людей і навіть усе людство. Надзвичайно цінна для одних користувачів інформація може не представляти цінності для інших.

Тому при організації захисту інформації визначають, насамперед, коло осіб (фірм, держав), які зацікавлені в даній інформації, так як імовірно, що серед них можуть бути зловмисники.

В інтересах захисту цінної (корисної) інформації її власник (держава, організація, фізична особа) наносить на носій умовний знак корисності інформації, яка міститься в ньому, — **гриф секретності** або конфіденційності.

Гриф секретності інформації, власниками якої є держава (державні органи), встановлюється на основі закону "Про державну таємницю" та відомчих переліків інформації, що складає державну таємницю.

Ціна інформації зв'язана з її цінністю, проте це різні поняття. Ціна інформації – це вартість інформації, виражена у грошових одиницях. Складається із собівартості інформації та прибутку від інформації.

Собівартість визначається витратами власника інформації на її одержання, наприклад:

- проведення досліджень в лабораторіях, аналітичних центрах, групах і т.ін.;
- купівля інформації;
- добування інформації за допомогою протиправних дій.

Прибуток від інформації може приймати різноманітні форми, не тільки грошовій. може бути одержаний в результаті наступних дій:

- продажу інформації;
- матеріалізації інформації в продукції з новими якостями або технології, що приносить прибуток;
- використання інформації для прийняття більш ефективних рішень.

1.3 Складові ціни інформації

Розповсюдження інформації та її використання призводять до змінювання її цінності та ціни. Характер зміни цінності у часі залежить від виду інформації. Для деякої інформації ця залежність часто має хвилеподібний характер.

Цінність більшості видів інформації, із часом зменшується — інформація старіє. За час життєвого циклу цінність інформації зменшується до 0,1 первісної величини. Залежно від тривалості життєвого циклу комерційна інформація звичайно класифікується наступним чином: – оперативно-тактична, яка втрачає цінність приблизно по 10% за день (наприклад, інформація видавання короткотривалого кредиту, пропозиції на придбання товару та строк до одного місяця і т.ін.); – стратегічна інформація, яка втрачає цінність приблизно по 10% за місяць (відомості про партнерів, про довготривалі кредити, розвиток підприємства та ін.)

При **копіюванні**, яке не змінює інформаційні параметри носія, кількість інформації не змінюється, а ціна зменшується. Після знімання копії з документа кількість інформації на ньому не змінюється Але якщо при копіюванні здійснюється вплив на інформаційні параметри носія, який призводить до зміни їхніх значень, або

незначні зміни нагромаджуються, то кількість інформації зменшується. (Погіршується якість звуку та зображення відповідно на аудіо- і відеоплівках через механічне руйнування магнітного шару, книга зачитується до дір, знебарвлюються через вплив яскравого ультрафіолетового світла колір зображення оригіналу при ксерокопіюванні та ін.) Так як при кожному копіюванні збільшується число її законних та незаконних користувачів, до відповідно до законів ринку ціна знижується. Інформація передається полем або речовиною. Це або акустична хвиля (звук), або електромагнітне випромінювання, або аркуш паперу з текстом тощо. Але ні передана енергія, ні передана речовина самі по собі ніякого значення не мають, вони є лише **носіями інформації**.

За фізичною природою можливі такі засоби перенесення інформації: – світлові промені; – звукові хвилі; – електромагнітні хвилі; – матеріали і речовини.

1.4 Види, джерела та носії інформації, що підлягає захисту

Інформація може бути з обмеженим доступом, що включає в собі державну таємницю, персональні дані, конфіденційну інформацію, іншу таємну інформацію, та відкриту інформацію.

Види інформації: - статистична інформація; - адміністративна інформація - масова інформація; - інформація про діяльність державних органів влади та органів місцевого самоврядування; - правова інформація; - інформація про особу; - інформація довідково-енциклопедичного характеру; - соціологічна інформація; - податкова інформація.

Носії інформації: - люди; - матеріальні тіла (макрочастки); - поля (випромінювання); - елементарні частки (мікрочастки). Так як за допомогою матеріальних засобів можна захищати тільки матеріальний об'єкт, то об'єктами захисту є матеріальні носії інформації.

Передавання інформації шляхом переміщення її носіїв у просторі зв'язана із затратами енергії, причому величина затрат залежить від довжини, шляху, параметрів середовища та виду носія. Джерела інформації: - документи всіх видів, на будь-яких видах носіїв; - персонал (пам'ять людей); - організаційні одиниці (кадрові, технічні, фінансові й інші ресурси); - промислові зразки, рецептури й технології, програмні засоби; - науковий інструментарій (автоматизовані робочі місця науковців і проектувальників, експертні системи і бази знань).

Інформація може бути:

- створеною її власником в результаті науково-дослідної діяльності,
- отримана внаслідок купівлі/продажу,
- запозичена з різноманітних відкритих джерел,
- може попасти до зловмисника випадково, наприклад, в результаті ненавмисного підслухування,
- і, нарешті, добута різноманітними нелегальними шляхами.

1.5 класифікація демаскуючих ознак об’єктів захисту

Демаскуюча ознака - властивість об'єкту відрізнятись за певними характеристиками від інших об'єктів. Відмінні характеристики можуть мати кількісну або якісну оцінку.

Технічна демаскуюча ознака об'єкту – характерна властивість об'єкту захисту, яке може бути використане технічною розвідкою для виявлення і розпізнавання об'єкту, а також для отримання необхідних відомостей про нього. Таким чином, доступ до інформації може бути здійснений шляхом аналізу демаскуючих ознак, що є по своїй суті своєрідними каналами витоку інформації (рис. 1.3):

- розташування – ознака що визначає положення об'єкту серед інших об'єктів і предметів навколишнього простору;

- структурно-видова - ознака, що визначає структуру і видові характеристики групового об'єкту (склад, кількість і розташування окремих об'єктів, форму і геометричні розміри);

- діяльності – ознака, що розкриває функціонування об'єкту через фізичні прояви.

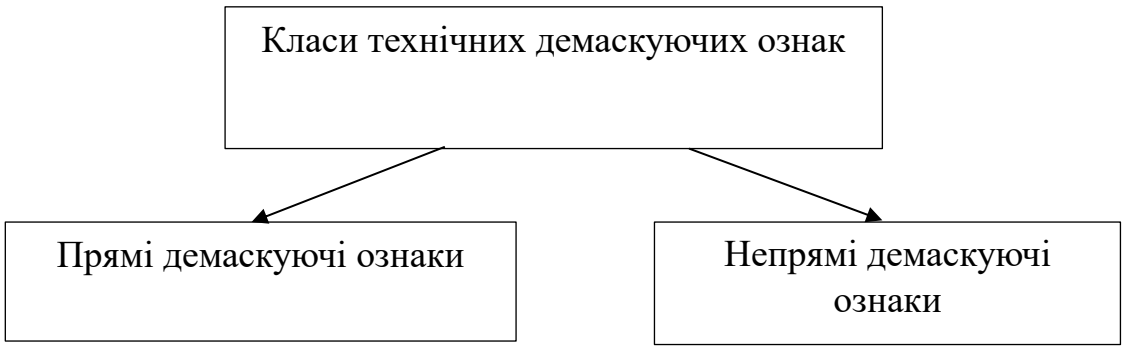

Рисунок 1.3 - Класифікацію демаскуючих ознак

Технічні демаскуючі ознаки можна розділити на два класи:

- прямі демаскуючі ознаки - ознаки, пов'язані з функціонуванням об'єкту захисту і що виявляються через їх фізичні поля (електромагнітні, акустичні, радіаційні і т.п.), що відрізняються по рівню на фоні фізичних полів навколишнього середовища, не пов'язаних із захищаємою інформацією;

- непрямі демаскуючі ознаки – ознаки у основі яких лежать наслідки зміни навколишнього середовища як результат функціонування об'єкту (візуально-оптичні ознаки діяльності, геометричні розміри, контрастність освітленості, сліди виробничої діяльності і функціонування і т.п.).

Завдання захисту ознакової інформації вирішується, насамперед, шляхом запобігання виявлення і розпізнавання об'єктів, що містять ці ознаки. Серед низки ознак властивих конкретному об'єкту, існують ознаки, які дозволяють виявляти його серед інших схожих об'єктів і розпізнати його приналежність, призначення, функції, властивості, особливості і характеристики.

Ознаки, що дозволяють відрізнити один об'єкт від іншого, називаються демаскуючими. Демаскуючі ознаки об'єкта складають частину його ознак, а значення їх відрізняються від значень відповідних ознак інших об'єктів. Співпадаючі значення ознак не відносяться до демаскуючих. Наприклад, ознака зріст людини без зазначення його значення не є демаскуючим, так як він ставиться до всіх людей. Під сигналом розуміється носій інформації у вигляді поля або потоку мікрочастинок.

Демаскуючі ознаки сигналів - це ознаки, за якими можна розпізнати об'єкт, який вони характеризують. Якщо необхідно запобігти можливість ідентифікації об'єкта, що захищається, то прояв демаскуючих ознак - є вразливість об'єкта, загроза його розпізнання потенційним зловмисником.

2. НЕБЕЗПЕЧНІ СИГНАЛИ ТА ЇХ ДЖЕРЕЛА

2.1. Поняття небезпечного сигналу.

2.2. Види побічних небезпечних електромагнітних випромінювань.

2.3. Небезпечні сигнали, що утворюються в результаті акустоелектичних перетворень.

2.4. Паразитні зв’язки та наведення.

2.5. Низько- та високочастотні випромінювання.

2.1 Поняття небезпечного сигналу

Фізичні явища, що лежать в основі появи випромінювань, мають різний характер, проте, в загальному вигляді просочування інформації за рахунок побічних випромінювань може розглядатися як ненавмисна передача конфіденційної інформації по деякій “побічній системі зв'язку”, що складається (рис 2.1):

- з передавача (джерела випромінювань),
- середовища, в якому ці випромінювання поширюються,
- приймаючої сторони.

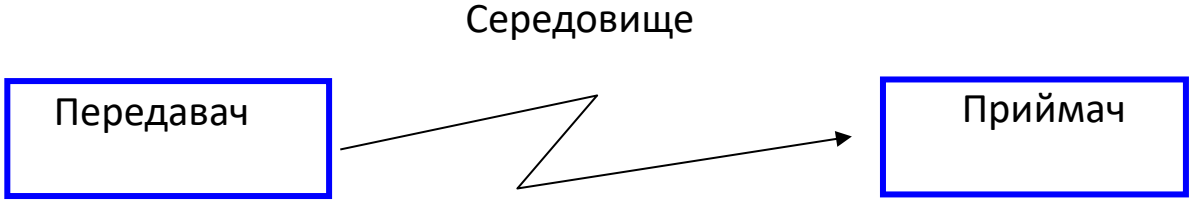

Рисунок 2.1 – Складові передачі повідомлення

При обробці засобами обчислювальної техніки конфіденційної інформації виникаючі побічні електромагнітні випромінювання є **небезпечними сигналами**. Небезпечні сигнали видобуваються шляхом прийому та аналізу їх при роботі

технічних засобів передачі, Обробки, зберігання та відображення інформації, і наводок що виникають у дротах, кабелях та інших токопровідних ланцюгах.

При цьому небезпечним вважають сигнал, якщо він містить конфіденційну інформацію і може бути перехоплений зловмисником. Небезпечні сигнали генеруються електронними пристроями обумовлені протіканням різноманітних видів струмів. При цьому існуючі системи передачі інформації можна поділити на 2 типи (рис 2.2).

В **не захищених** системах зв'язку, в яких передаюча і приймаюча сторони, переслідують одну мету — передати інформацію з найбільшою достовірністю

При **захищеній** передачі сторона, що “передає”, навпаки зацікавлена у можливому погіршенні передачі інформації, оскільки це сприяє її захисту.

Описану “систему зв'язку” прийнято називати ***технічним каналом просочування інформації***.

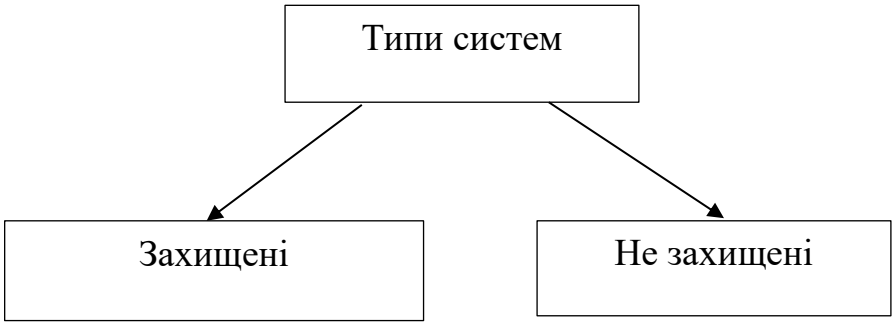

Рисунок 2.2 – Типи систем зв'язку

Також при обміні даними необхідно врахувати наявність у навколишньому середовищі багаточисельних перешкод як природного, так і штучного походження, які істотним чином впливають на можливості прийому.

2.2 Види побічних небезпечних електромагнітних випромінювань

Під час пересилання інформації з обмеженим доступом в елементах схем, конструкцій, підвідних і з’єднувальних проводах технічних засобів протікають струми інформативних (небезпечних) сигналів (рис. 2.3).

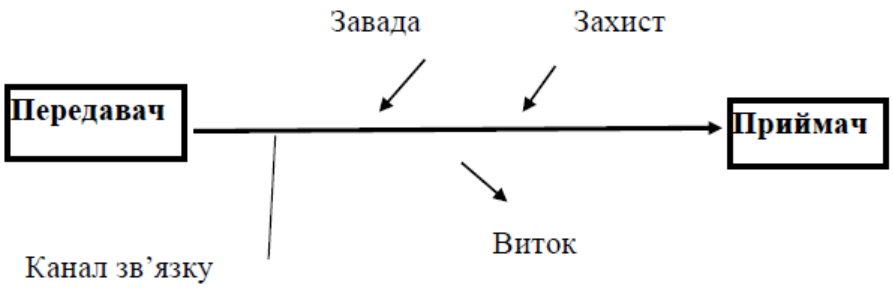

Рисунок 2.3 – Передача сигналу по каналам зв’язку

Окрім того **джерелами небезпечних сигналів** є елементи, вузли а також

токопровідні ланцюги різноманітних технічних засобів зі струмами та напругами небезпечних сигналів. Причому, ці пристрої генерують як магнітні, так і електромагнітні поля в широкому частотному спектрі, характер яких визначається призначенням, схемними рішеннями, потужністю пристрою, а також його конструкцією.

Електромагнітні випромінювання: носієм інформації є електричний струм, сила якого, напруга, частота або фаза змінюються за законом інформаційного сигналу. Електромагнітні випромінювання на частотах роботи високочастотних генераторів, що входять до складу обладнання: в результаті дії інформаційного сигналу на елементах генераторів наводяться електричні сигнали, які можуть викликати ненавмисну модуляцію власних високочастотних коливань генераторів і випромінювання в навколишній простір. Електромагнітні випромінювання на частотах самозбудження підсилювачів низької частоти технічних засобів передачі інформації: самозбудження можливе за рахунок випадкових перетворень від'ємних зворотних зв'язків у паразитні додатні, що приводить до переведення підсилювача з режиму підсилення в режим автогенерації сигналів, причому сигнал на частотах самозбудження, як правило, виявляється промодульованим інформаційним сигналом.

2.3 Небезпечні сигнали, що утворюються в результаті акустоелектичних перетворень

Окрему загрозу витоку інформації за електромагнітним каналом створюють засоби аудіофікації приміщень (мікрофони, підсилювачі потужності, гучномовці) , під час озвучення захищуваної інформації. Найбільшу небезпеку створюють підсилювачі потужності систем аудіофікації за їх монтажу в віддаленому від ОІД технічному приміщенні та, як наслідок цього, з наявністю довгих з'єднувальних кабелів з протікаючими ними струмами значної величини. Створювані струмами потужні магнітні поля не тільки самостійно поширюються в навколишньому середовищі на значну відстань, так і є причиною наведення вторинної е.р.с. у навколишніх струмопровідних конструкціях та ланцюгах електроживлення апаратури об'єкту інформаційної діяльності.

Акустоелектричні канали витоку інформації виникають за рахунок перетворень акустичних каналів в електричні. Деякі елементи допоміжних технічних засобів і систем (ДТЗС), у тому числі трансформатори, котушки індуктивності, електромагніти вторинних годиників, телефонних дзвінків апаратів і тощо, мають властивість змінювати свої параметри (ємність, індуктивність, опір) під дією акустичного поля, створюваного джерелом мовного сигналу.

Зміна параметрів призводить або до появи на даних елементах електрорушійної сили (ЕРС), або до модуляції струмів, що протікають по цим елементам згідно із змінами електричного поля.

ДТЗС, крім зазначених елементів, можуть містити безпосередньо акустоелектричні перетворювачі. До таких відносяться деякі типи датчиків пожежної та охоронної сигналізації, гучномовці ретрансляційної мережі тощо.

Ефект акустоелектричного перетворення іноді називають «мікрофонним ефектом». Перехоплення акустоелектричних коливань в даному каналі витоку інформації здійснюється шляхом безпосереднього підключення до з'єднувальних ліній ДТЗС спеціальних високочутливих УНЧ.

2.4 Паразитні зв’язки та наведення

Елементи, ланцюги, тракти, дроти сполучення і лінії зв'язку будь-яких електронних систем і схем постійно знаходяться під впливом власних (внутрішніх) і сторонніх (зовнішніх) електромагнітних полів різного походження, що індукують або наводять в них значну напругу. Таку дію називають електромагнітним впливом або просто впливом на елементи ланцюга. Паразитні ємкісні зв'язки обумовлені електричною ємкістю, що утворюється між елементами, деталями і провідниками схем (рис. 2.4).

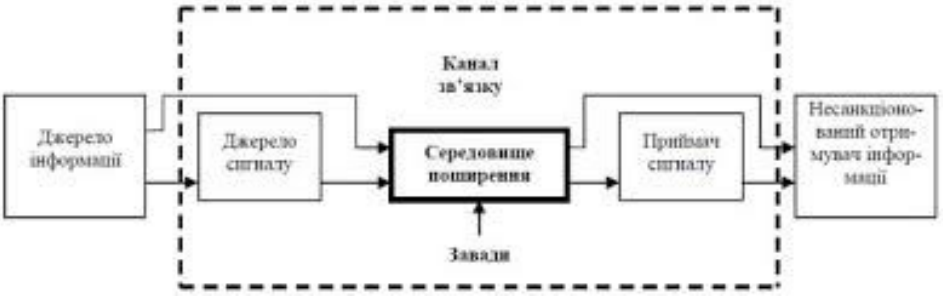

Рисунок 2.4 – Утворення паразитних ємкісніх зв'язків

Оскільки опір ємності, що створює паразитний ємнісний зв'язок, падає із зростанням частоти (X = 1/Cw), то енергія, що виділяється, з підвищенням частоти збільшується. Тому паразитний ємнісний зв'язок може привести до самозбудження підсилювача на частотах, що перевищують його вищу робочу частоту.

Паразитні індуктивні зв'язки обумовлені наявністю взаємоіндукції між провідниками і деталями РЕО, головним чином між її трансформаторами. Паразитний індуктивний зворотний зв'язок між трансформаторами підсилювача — наприклад, між вхідним і вихідним трансформаторами, — може викликати режим самозбудження в області робочих частот і на гармоніках.

Паразитні електромагнітні зв'язки приводять до самозбудження окремих каскадів звукових і широкосмугових підсилювачів на частотах порядка десятки і сотні мегагерц. Ці зв'язки зазвичай виникають між вихідними провідниками підсилювальних елементів, створюючи коливальну систему з розподіленими параметрами і резонансною частотою певного діапазону.

2.5 Низько- та високочастотні випромінювання

Технічні канали витоку інформації звичайно утворюються (рис. 2.5):

- виникаючими під час роботи ТЗПІ і допоміжних технічних засобів та систем (ДТЗС) низькочастотними електромагнітними полями;
- за зовнішнього впливу на ТЗПІ і ДТЗС електричних, магнітних і акустичних полів;
- при збудженні паразитної високочастотної генерації в колах підсилювачів сигналів;
- при просоченні інформативних сигналів ланцюгами електроживлення;
- за взаємного впливу електричних ланцюгів;
- при просоченні інформативних сигналів ланцюгами заземлення;
- внаслідок проведення помилкових комутацій і інших несанкціонованих дій.

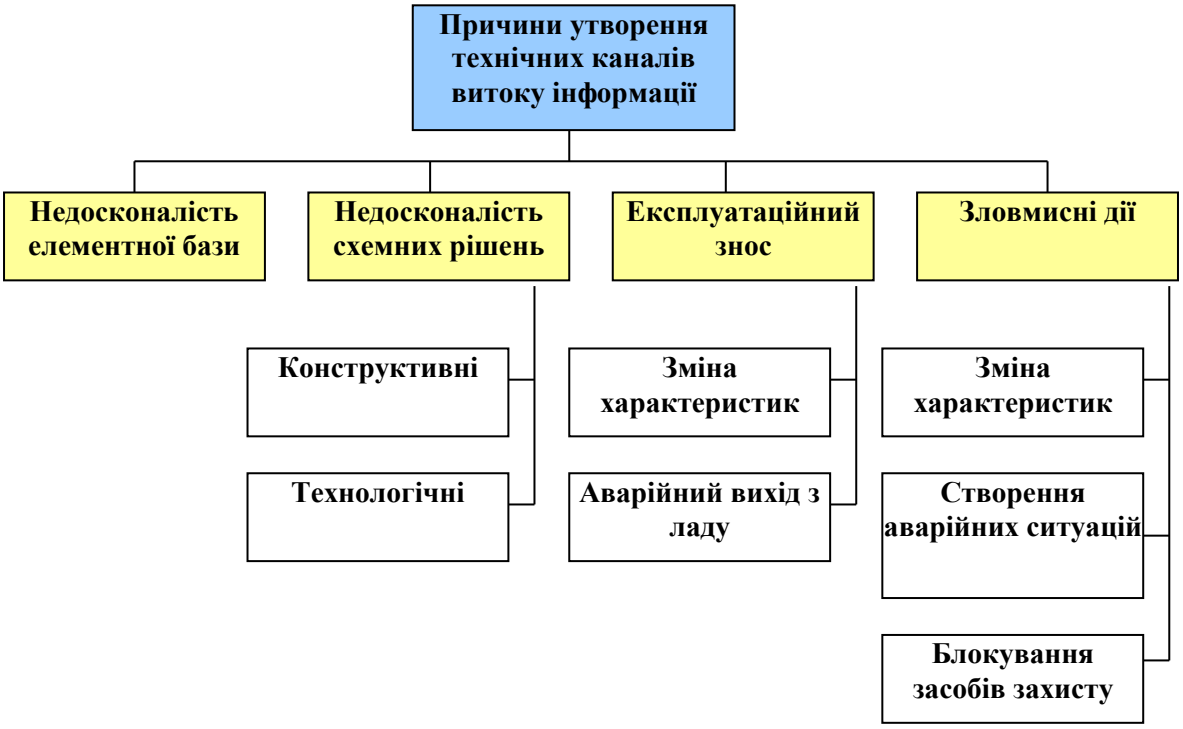

Рисунок 2.5 – Причини утворення технічних каналів витоку інформації

Технічний канал витоку інформації з використанням «високочастотного електромагнітного нав'язування» може бути здійснено шляхом несанкціонованого контактного введення струмів високої частоти від генератора в лінію, що має функціональні зв'язки з нелінійними або параметричними елементами ДТЗС, на яких відбувається модуляція високочастотного каналу інформаційним сигналом (рис. 2.6). Зовнішній вплив електромагнітних коливань інформаційного сигналу на елементи високочастотних генераторів (що входять до складу апаратури ТЗПІ та ДТЗС) може спричиняти побічну небажану модуляцію власних коливань ВЧ генераторів з наступним випромінюванням цих модульованих ВЧ-коливань у навколишній простір.

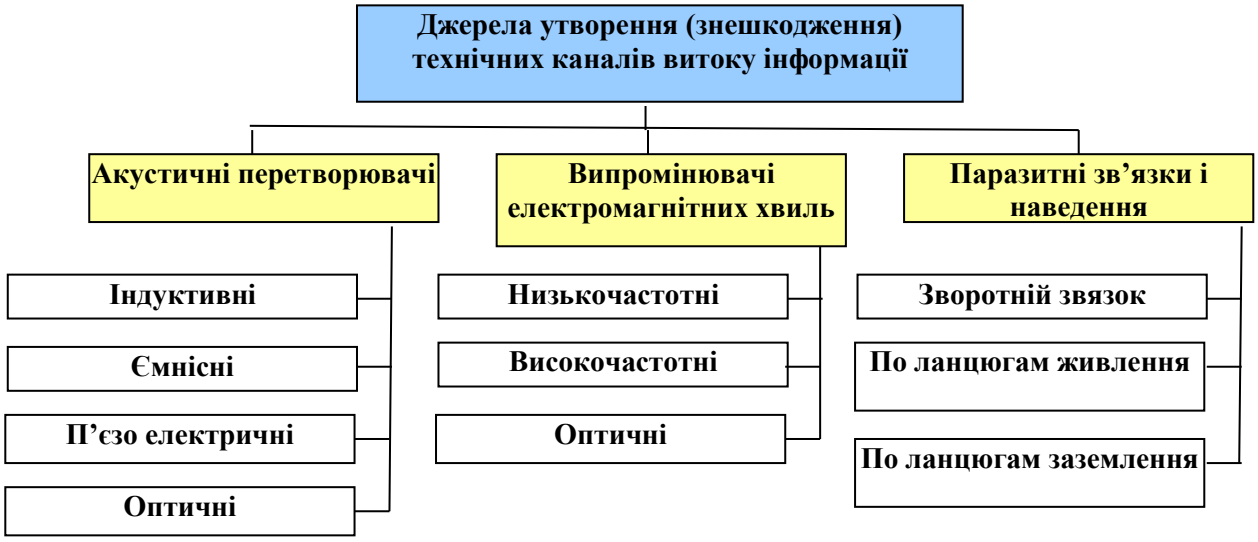

Рисунок 2.6 – Причини утворення технічних каналів витоку інформації

Виникнення промодульованих ВЧ-коливань також можливе за умови самозбудження підсилювачів сигналів низької частоти ТЗПІ в системах гучномовного оповіщення та зв'язку, що виникає за умови паразитних зворотних зв'язків, переводячи підсилювачі НЧ у режим автогенератора. При цьому сигнал самозбудження виступає несучою частотою, промодульованою інформаційним сигналом.

3 ТЕХНІЧНА РОЗВІДКА

3.1 Поняття та принципи технічної розвідки.

3.2 Основні задачі та органи технічної розвідки.

3.3 Види технічної розвідки.

3.4 Поняття промислового шпигунства.

3.5 Законні та незаконні методи добування конфіденційної інформації про діяльність конкурентів.

3.6 Контррозвідувальна діяльність.

3.7 Комплексний захист конфіденційної інформації, його види.

3.8 Пасивні та активні методи захисту конфіденційної інформації.

3.1 Поняття та принципи технічної розвідки

Технічна розвідка (ТР) - несанкціоноване здобування секретної інформації за допомогою технічних засобів та її аналіз.

Мета ТР - забезпечення вищого політичного керівництва своєї держави своєчасною інформацією, по її Збройних Силах (ЗС), по військово-економічному потенціалі.

Основні об'єкти ТР: - ЗС, - оборонна промисловість, - науково-дослідні центри, - полігони, транспорт, - зв'язок, - енергосистеми, - системи охорони найбільш важливих урядових і військових об'єктів.

Принципи організації ТР (рис. 3.1): - Цілеспрямованість означає, що вся діяльність по добуванню інформації різних іноземних спецслужб поєднується в рамках різного роду сполучників і направляється в основному проти нашої країни; - Централізація керівництва полягає в напрямку вищим політичним керівництвом країни розвідницької діяльності спецслужб різної відомчої приналежності; - Розміщення технічних засобів на границі уздовж території нашої країни припускає використання для збору інформації території суміжних з нашою країною держав, водних акваторій, що прилягають до наших територіальних вод, маршрутів польоту через територію нашої країни літаків іноземних авіакомпаній, а також будинків посольств, консульств, торговельних представництв іноземних держав у нашій країні.

Рисунок 3.1 – Принципи технічної розвідки

Використання для збору інформації нерозвідувальних систем і засобів припускає залучення для збору інформації ряду відомчих нерозвідувальних систем:

- командні вимірювальні комплекси ракетних полігонів;
- науково-дослідні технічні станції;
- системи раннього попередження про ракетно-ядерний напад;
- штучні супутники Землі, призначені для геофізичних досліджень;
- пасажирські літаки іноземних авіакомпаній, судна торговельного, рибальського й пасажирського флотів.

Принципи ведення ТР:

- Комплексність означає, що для збору інформації про конкретні об’єкти використовується набір розвідувальної апаратури, що одержує інформацію з різних фізичних полів, створюваних об’єктами розвідки, дублювання даних для підвищення достовірності;

- Оперативність означає, що розвідувальні завдання вирішуються в мінімально короткі строки.

- Безперервність полягає в тому, що збір інформації виконується постійно, у будь-яких умовах і при будь-яких обставинах незалежно від пори року, доби, погоди, будь-яких умов обстановки;

- Глобальність полягає в тому, що розвідувальна діяльність охоплює значні території земної кулі;

- Плановість полягає в тому, що вся діяльність по збору інформації за допомогою ТР виконується відповідно до заздалегідь розроблених програм;

- Прихованість полягає у використанні для збору інформації апаратури пасивного типу, у маскуванні й камуфлюванні апаратури при веденні розвідки, у широкому використанні заходів щодо засекречування й легендуванню розвідувальних операцій, приховування фактів витоку або зміни інформації

3.2 Основні задачі та види технічної розвідки

Завданням ТР є збір інформації:

- зі стану й перспектив розвитку військово-економічного потенціалу країни,

- по складу, чисельності, дислокації й технічній оснащеності військ і сил флоту,

- по стані бойової готовності ЗС,

- по розміщенню на території країни об’єктів оборонної промисловості, що випускається ними продукції, виробничої потужності,

- по найбільш важливих розробках в області озброєння й військової техніки,

- по ефективності існуючого й розроблювального озброєння,

- по проведених навчаннях військ і сил флоту, по ступені підготовки території країни до ведення бойових дій,

- по наявності паливно-енергетичних, рудних, водних і ін. ресурсів країни.

Різноманіття видів носіїв інформації породило безліч видів технічної розвідки. Її класифікують за різними ознаками (підставами класифікації). Найбільш широко застосовуються дві класифікації: по фізичній природі носіїв інформації і за способами ведення та каналами добування інформації(рис 3.2).

У збройних силах провідних держав світу прийнято на озброєння сучасні прилади (системи) розвідки та цілевказування, які забезпечують ведення оптичної розвідки, передачу інформацію про цілі в реальному масштабі часу, здійснення корегування артилерійського вогню та ударів авіації, управління високоточними боєприпасами.

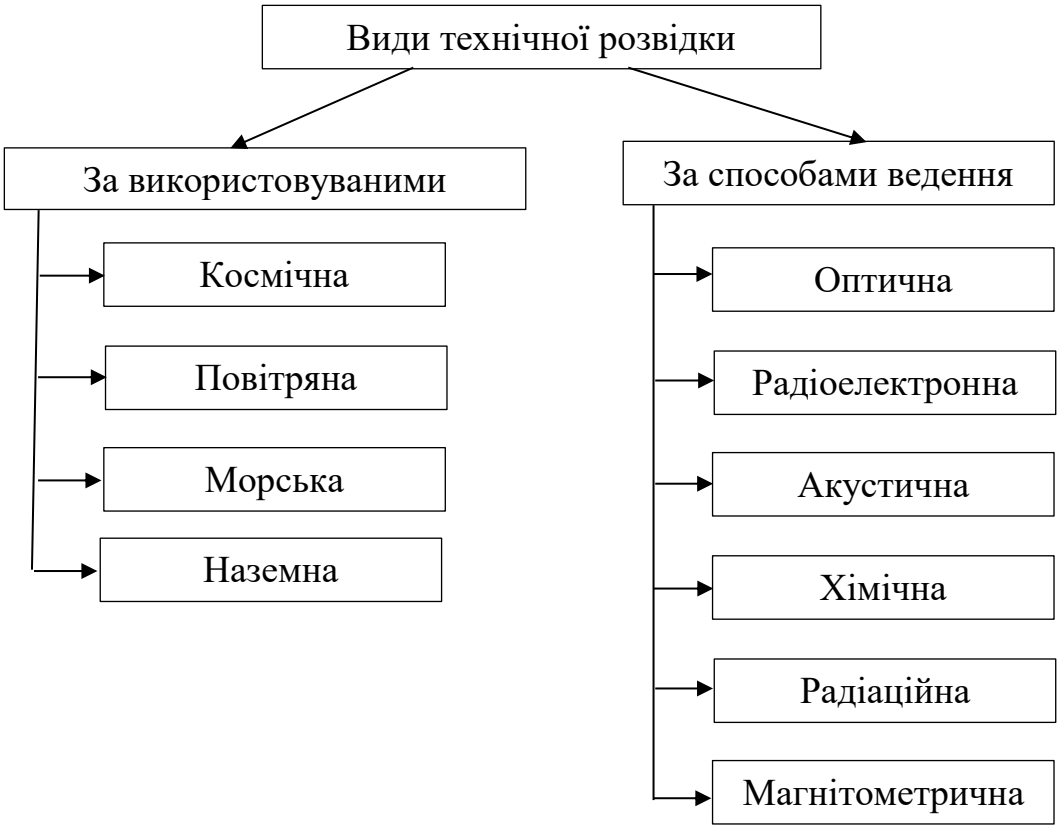

Рисунок 3.2 – Види технічної розвідки

Оптична розвідка включає:

- візуально-оптичну,
- фотографічну,
- інфрачервону,
- телевізійну,
- лазерну.

Радіоелектронна розвідка в залежності від характеру добувної інформації підрозділяється на:

- - радіорозвідку;
- - радіотехнічну розвідку;
- - радіолокаційну розвідку;
- - радіотеплового розвідку;
- - комп'ютерну розвідку.

Хімічна розвідка добуває інформацію про склад, структуру та властивості речовин шляхом взяття проб і аналізу їх макрочасток. Хімічна розвідка - це комплекс заходів, спрямованих на виявлення зараження отруйними речовинами місцевості у районах розташування та на напрямках дії військ, що проводяться з метою попередження ураження особового складу хімічною зброєю.

Вимоги до хімічної розвідки: своєчасність; безперервність; достовірність; спадкоємність.

Радіаційна розвідка призначена для виявлення, локалізації, визначення

характеристик і вимірювання рівнів випромінювання радіоактивних речовин.

Радіаційна розвідка є важливим заходом у системі захисту особового складу військ від ядерної зброї і проводиться з метою своєчасного виявлення і попередження підрозділів про радіоактивне зараження місцевості.

Радіаційна розвідка проводиться у підрозділах і частинах усіх родів військ і організовується командирами (начальниками) всіх ступенів та штабами.

Вимоги до радіаційної розвідки - безперервність, достовірність, спадкоємність, своєчасність сповіщення про радіоактивне забруднення місцевості.

За способом ведення радіаційна розвідка може бути наземною і повітряною.

Магнітометрична розвідка дозволяє по зміні магнітного поля Землі виявляти тіла, які мають власне магнітне поле, наприклад, підводні човни в зануреному стані.

Магніторозвідка — група геофізичних методів розвідки, що базуються на вивченні магнітного поля Землі. Полягають у виявленні й вивченні магнітних аномалій, які виникають внаслідок неоднакового намагнічення різних гірських порід. Елементи магнітного поля на земній поверхні та під нею вимірюють магнітометрами, у повітрі — аеромагнітометрами з літаків та вертольотів.

Розрізняють наземну, аеромагнітну, авіадесантну, підземну, гідромагнітну зйомки; магнітні виміри в свердловинах; лабораторні магнітні виміри магнітних варіацій та метод штучного підмагнічування порід.

Результати зйомки наносять на карти, аномальне значення магнітного поля Землі зображують у вигляді ізоліній або графіків.

М. м. р. у комплексі з ін. методами застосовують для дослідження геол. будови земної кори, розшуків і розвідки корисних копалин.

Акустична розвідка в залежності від середовища поширення акустичному хвилі ділиться на повітряно-акустичну, гідроакустичну і сейсмічну.

Звукова розвідка (також Артилерійська звукова розвідка, АЗР) — складова артилерійської розвідки.

Звукометрія — розділ прикладної акустики з визначення місце знаходження артилерійської зброї за звуком пострілу.

3.3 Поняття промислового шпигунства законні та незаконні методи добування конфіденційної інформації про діяльність конкурентів

Комерційна розвідка — це діяльність, спрямована на забезпечення і підтримку стратегії успішного ведення справ комерційного підприємства, яка здійснюється з метою досягнення переваги над потенційним конкурентом, а також виявлення нових можливостей і ділових ризиків — ось найбільш правильне визначення.

Комерційна розвідка займається:

- вивченням і виявленням організацій, що потенційно є союзниками або конкурентами;

- добуванням, збирають і опрацьовують дані про діяльність потенційних і реальних конкурентів;

- обліком і аналізом спроб несанкціонованого отримання комерційних секретів конкурентами;

- оцінкою реальних відносин між співпрацюють і конкурують організаціями;

- аналізом можливих каналів витоку конфіденційної інформації.

Активний метод комерційної розвідки дуже часто (і не без підстав) відносять до методів промислового шпигунства, проте саме він і надає основні конкурентні переваги підприємству здійснює розвідку, так як незаперечна істина, що найкращий захист це напад.

Сукупно-пасивний метод — цей процес передбачає взаємодію з вторинними джерелами інформації (реклама, ЗМІ, документи), і поєднання їх з активними діями (агентура, стеження).

Сукупність методів, притаманних промисловому шпигунству, можна об'єднати у дві групи:

1. Агентурні методи.

2. Технічні методи.

Агентурний метод одержання інформації — основа основ будь-якого виду шпигунства. Тут можливі два напрями діяльності: або вербування, або впровадження своєї людини.

На противагу промисловому шпигунству, **конкурентна розвідка** - постійний процес збору, нагромадження, структурування, аналізу даних про внутрішнє й зовнішнє середовище компанії й надання вищому менеджменту компанії інформації, що дозволяє йому передбачати зміни в обстановці й приймати своєчасні оптимальні рішення щодо управління ризиками, впровадження змін у компанії й відповідних заходів, спрямованих на задоволення майбутніх запитів споживачів і підтримку прибутковості. Важливим є та обставина, що конкурентна розвідка здійснює збір інформації про навколишнє бізнес-середовище тільки законними методами.

Методи конкурентної розвідки умовно можна поділити на цілком законні (білі) та методи, які за своєю формою не порушують норм законів, проте не завжди відповідають морально-етичним нормам ведення чесної конкурентної боротьби (сірі методи).

До **першої** групи методів конкурентної розвідки, тобто до законних, належать:

- вивчення й аналіз публікацій конкурента;

- вивчення, аналіз та обробка відкритої інформації про конкурента.

До **другої** групи методів належать такі:

- матеріальне заохочення співробітників конкурента з метою отримання конфіденційної інформації;

- «переманювання» спеціалістів конкурента і отримання в них відомостей, що мають обмежений доступ;

- вивідування інформації у співробітника конкурента;

- проведення підставних переговорів з метою вивідування конфіденційної інформації;

- отримання необхідної інформації про конкурента через зв'язки в правоохоронних та контролюючих органах.

3.4 Контррозвідувальна діяльність

Контррозвідувальна діяльність - спеціальний вид діяльності у сфері забезпечення державної безпеки, яка здійснюється з використанням системи контррозвідувальних, пошукових, режимних, адміністративно-правових заходів, спрямованих на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України.

Метою контррозвідувальної діяльності є попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, припинення розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що їм сприяють, та причин їх виникнення.

Завданнями контррозвідувальної діяльності є: - добування, аналітична обробка та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України; - протидія розвідувальній, терористичній та іншій діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України; - розроблення і реалізація заходів щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян.

Основними **принципами** контррозвідувальної діяльності є: - законність; - повага і дотримання прав та свобод людини і громадянина; - позапартійність; - безперервність; - конспірація, поєднання гласних та негласних форм і методів діяльності; - комплексне використання правових, профілактичних та організаційних заходів; - адекватність заходів щодо захисту державної безпеки реальним і потенційним загрозам; - взаємодія з органами державної влади України, органами місцевого самоврядування, об'єднаннями громадян, юридичними та фізичними особами; - підконтрольність та підзвітність відповідним органам державної влади в межах, передбачених законом.

3.5 Комплексний захист конфіденційної інформації, його види

Комплексна система захисту інформації (КСЗІ) — взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Одним з напрямків захисту інформації в комп'ютерних системах є **технічний захист інформації** (ТЗІ).

В свою чергу, питання ТЗІ розбиваються на два великих класи задач: - захист інформації від несанкціонованого доступу (НСД) - захист інформації від витоку технічними каналами.

Для забезпечення ТЗІ створюється комплекс технічного захисту інформації, що є складовою КСЗІ.

Під НСД звичайно розуміється доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу.

Під технічними каналами розглядаються канали побічних електромагнітних випромінювань і наводок (ПЕМВН), акустичні канали, оптичні канали та інші.

Захист від НСД може здійснюватися в різних складових інформаційної системи:

- прикладне та системне ПЗ.
- апаратна частина серверів та робочих станцій.
- комунікаційне обладнання та канали зв'язку.
- периметр інформаційної системи.

Для захисту інформації на рівні прикладного та системного ПЗ нами використовуються: - системи розмежування доступу до інформації; - системи ідентифікації та автентифікації; - системи аудиту та моніторингу; - системи антивірусного захисту.

Захист інформації від її витоку технічними каналами зв'язку забезпечується такими засобами та заходами: - використанням екранованого кабелю та прокладка проводів та кабелів в екранованих конструкціях; - встановленням на лініях зв'язку високочастотних фільтрів; - побудовою екранованих приміщень («капсул»); - використанням екранованого обладнання; - встановленням активних систем зашумлення; - створенням контрольованої зони.

4 КОНЦЕПЦІЯ І МЕТОДИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

1. Комплексне застосування методів захисту.
2. Основні напрямки інженерно-технічного захисту інформації.
3. Методи фізичного захисту інформації.
4. Просторове та структурне приховування інформації.
5. Часове та енергетичне приховування інформації.
6. Поняття інформаційного портрету та інформаційного вузла об’єктів захисту.
7. Дезінформація, як метод захисту інформації.

4.1 Комплексне застосування методів захисту

Сукупність методів і засобів захисту інформації включає:

- апаратні засоби;

- програмні засоби;
- захисні перетворення;
- організаційні заходи.

Апаратний, або схемний, захист полягає в тому, що в приладах ЕОМ та інших технічних засобах обробки інформації передбачається наявність спеціальних схем, що забезпечують захист і контроль інформації, наприклад, схеми контролю на чесність, які контролюють правильність передачі інформації між різними приладами ЕОМ, а також екрануючими приладами, що локалізують електромагнітні випромінювання.

Програмні методи захисту — це сукупність алгоритмів і програм, які забезпечують розмежування доступу та виключення несанкціонованого використання інформації.

Сутність методів **захисних перетворень** полягає в тому, що інформація, яка зберігається в системі та передається каналами зв'язку, подається в деякому коді, що виключає можливість її безпосереднього використання.

Організаційні заходи із захисту інформації містять сукупність дій з підбору та перевірки персоналу, який бере участь у підготовці й експлуатації програм та інформації, чітке регламентування процесу розробки та функціонування інформаційної системи. Лише комплексне використання різних заходів може забезпечити надійний захист інформації, тому що кожний метод або захід має слабкі та сильні сторони.

Концепція захисту інформації - офіційно прийнята система поглядів на проблему інформаційної безпеки і шляхи її вирішення з урахуванням розробки сучасних тенденцій (рис. 4.1).

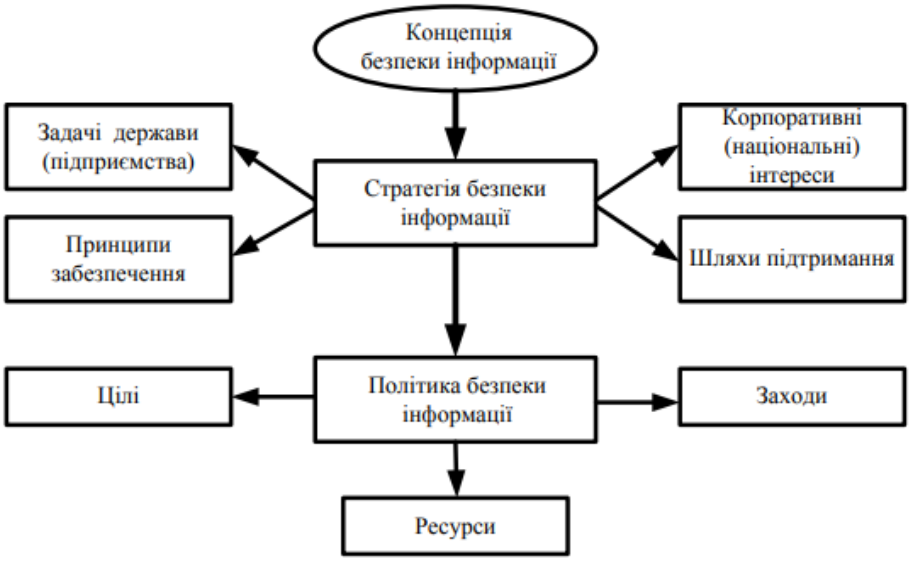

Рисунок 4.1 – Концепція захисту інформації

Вона є методологічною основою політики розробки практичних заходів її реалізації. Розробку концепції захисту проводять в три етапи (рис. 4.2):

Рисунок 4.2 – Етапи розробки концепції захисту

На **першому етапі** чітко визначається цільова установка захисту, тобто які реальні цінності, виробничі процеси, програми, масиви даних необхідно захищати. На даному етапі доцільно диференціювати, за значимістю, окремі об’єкти, які підлягають захисту.

Другий етап. Проведення скурпульозного аналізу злочинних дій, які потенційно можуть бути здійснені стосовно об’єкту, котрий слід захистити. Важливо визначити ступінь реальної небезпеки найбільш поширених злочинів та проаналізувати ймовірні дії зловмисників стосовно об’єктів, які потребують захисту.

Головною метою **третього етапу** є аналіз обставин, в тому числі місцевих специфічних умов, виробничих процесів, уже встановлених технічних засобів захисту. Концепція захисту повинна містити перелік організаційних, технічних та інших заходів, які забезпечують максимальну безпеку при заданому залишковому ризику при мінімальних затратах на їх реалізацію.

4.2 Основні напрямки інженерно-технічного захисту інформації

До інженерно-технічних заходів можна віднести захист від несанкціонованого доступу до КС, резервування важливих комп’ютерних блоків і систем, резервне електроживлення, розробку та реалізацію спеціальних програмних і апаратних комплексів тощо. Фізичні засоби містять у собі різні інженерні засоби, які перешкоджають фізичному проникненню зловмисників на об’єкти захисту, які захищають персонал, матеріальні засоби і фінанси, інформацію про протиправні дії.

Теорія інженерно-технічного захисту інформації описує основні принципи, засоби і методи забезпечення інформаційної безпеки об'єктів (рис. 4.3).

Інженерно-технічний захист складається з таких компонентів, як спеціальні органи, технічні засоби та заходи щодо їх використання для захисту конфіденційної інформації. Постійна і ефективна технічна захист інформаційних ресурсів є обов'язковою складовою комплексної системи забезпечення інформаційної безпеки і сприяє оптимізації грошових витрат на організацію захисту інформації.

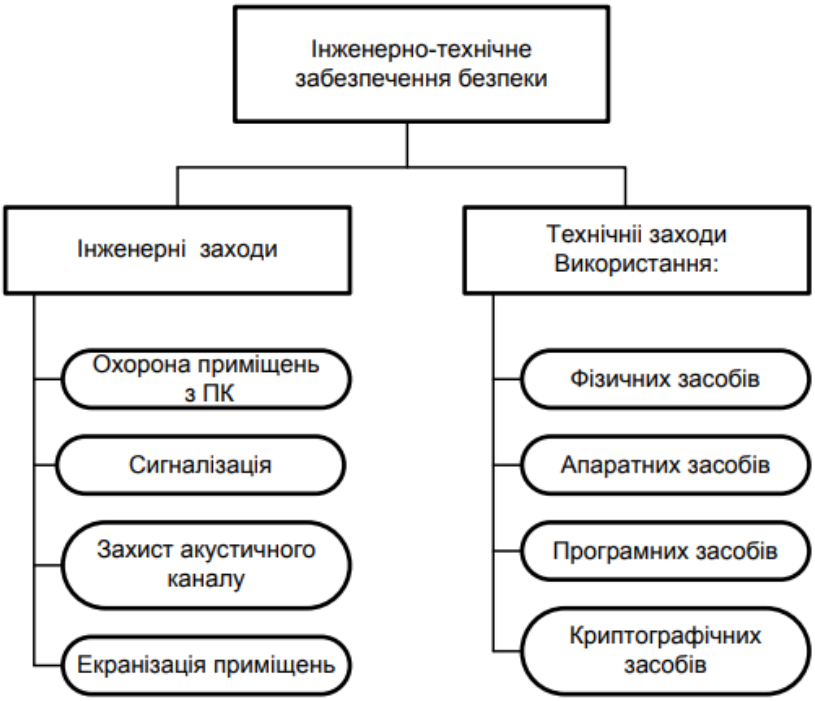

Рисунок 4.3 – Етапи розробки концепції захисту

Технічний захист інформації передбачає цілий комплекс заходів щодо захисту інформації від несанкціонованого доступу з різних видів каналів, а також виключення спеціальних впливів на неї, таких як, знищення, перекручення або блокування доступу.

4.3 Методи фізичного захисту інформації

Фізичні засоби захисту - різноманітні пристрої, пристосування, конструкції, апарати, вироби, призначені для створення перешкод на шляху руху зловмисників. До фізичних засобів відносяться механічні, електромеханічні, електронні, електронно-оптичні, радіо- та радіотехнічні та інші пристрої для заборони несанкціонованого доступу (входу-виходу), проносу (виносу) засобів і матеріалів та інших можливих видів злочинних дій.

Ці засоби застосовуються для вирішення наступних завдань:

- Охорона території підприємства і спостереження за нею.
- Охорона будівель, внутрішніх приміщень і контроль за ними.
- Охорона обладнання, продукції, фінансів та інформації.
- Здійснення контрольованого доступу до будівлі та приміщення.

Всі фізичні засоби захисту об'єктів можна розділити на три категорії: засоби попередження, засоби виявлення та системи ліквідації загроз.

Охоронна сигналізація і охоронне телебачення, наприклад, відносяться до засобів виявлення загроз; паркани навколо об'єктів - це засоби попередження несанкціонованого проникнення на територію, а посилені двері, стіни, стелі, грати

на вікнах та інші заходи служать захистом і від проникнення і від інших злочинних дій. Засоби пожежогасіння відносяться до систем ліквідації загроз.

4.4 Просторове та структурне приховування інформації

Головний спосіб протидії **технічним засобам розвідки** (ТЗР) є приховування **джерела повідомлення** (ДП), в процесі якого шляхом проведення організаційних і технічних заходів досягається мета виключення або істотного ускладнення виявлення ДП. Приховування інформації (хования, приховування) об'єднує групу методів захисту інформації, основу яких складають умови і дії, що ускладнюють пошук і виявлення об'єктів захисту, розпізнавання та вимірювання їх ознак, зняття з носіїв інформації з якістю, достатньою для її використання. Воно передбачає зміни місця розташування, часу передачі повідомлення або прояви демаскуючих ознак, структури інформації, структури і енергії носіїв, при яких зловмисник не може безпосередньо або за допомогою технічних засобів виділити інформацію з якістю, достатньою для використання її у власних інтересах. Приховувати від зловмисника можна як інформацію, так і її носій. Розрізняють просторове, тимчасове, структурне і енергетичне приховування (рис. 4.4).

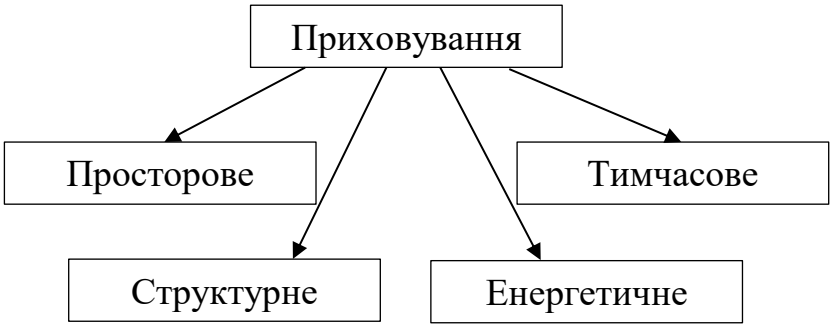

Рисунок 4.4 – Типи приховування

Просторове приховування ускладнює пошук і виявлення зловмисником джерела інформації в просторі. Воно досягається розміщенням джерела інформації в місцях, розташування яких апріорі зловмиснику не відомо. Такі місця зберігання називаються секретами. Перед зловмисником виникає додаткове завдання - пошук джерела. Чим більше область пошуку, тим важче знайти об'єкт. До просторових можна віднести стеганографічні способи захисту інформації, які передбачають потайне розміщення інформації, що захищається, яка відображається в символьній формі, в так званих контейнерах.

4.5 Часове та енергетичне приховування інформації

Енергетичне приховування досягається зменшенням відносини енергії (потужності) сигналів, та носіїв (електромагнітного або акустичного полів і електричного струму) з інформацією, і перешкод. Зменшення відносини сигнал /

перешкода (слово «потужність», як правило, опускається) можливо двома методами: зниженням потужності сигналу або збільшенням потужності перешкоди на вході приймача. Вплив перешкод призводить до зміни інформаційних параметрів носіїв: амплітуди, частоти, фази.

Якщо носієм інформації є амплітудно змодульована електромагнітна хвиля, а в середовищі поширення каналу присутній перешкода у вигляді електромагнітної хвилі, що має однакову з носієм частоту, але випадкову амплітуду і фазу, то відбувається інтерференція цих хвиль. В результаті цього значення інформаційного параметра (амплітуди сумарного сигналу) випадковим чином змінюються і інформація спотворюється. Чим менше відношення потужностей, а отже, амплітуд, сигналу і перешкоди, то більша значення амплітуди сумарного сигналу будуть відрізнятися від вихідних (встановлюються при модуляції) і тим більше буде спотворюватися інформація.

4.6 Поняття інформаційного портрету та інформаційного вузла об’єктів захисту

Інформаційним портретом можна назвати сукупність елементів і зв'язків між ними, що відображають зміст повідомлення, ознаки об'єкта чи сигналу. Елементами дискретного семантичного повідомлення, наприклад, є літери, цифри та інші знаки, а зв'язки між ними визначають їх послідовність. Інформаційними портретами об'єктів спостереження, сигналів і речовин є їх еталонні признакові структури.

Можливі такі способи зміни інформаційного портрета:

- Видалення частини елементів і зв'язків, що утворюють інформаційний вузол (найбільш інформативну частину) портрета;
- Зміна частини елементів інформаційного портрета при збереженні незмінності зв'язків між рештою елементами;
- Видалення або зміна зв'язків між елементами інформаційного портрета при збереженні їх кількості.

Зміна інформаційного портрета об'єкта викликає зміна зображення його зовнішнього вигляду (видових демаскуючих ознак), характеристик випромінюваних їм полів або електричних сигналів (ознак сигналів), структури і властивостей речовин. Ці зміни спрямовані на зближення признакових структур об'єкта і навколишнього його тла, в результаті чого знижується контрастність зображення об'єкта по відношенню до фону і погіршуються можливості його виявлення і розпізнавання.

4.7 Дезінформація, як метод захисту інформації

Дезінформування найбільш ефективно при приховуванні семантичної інформації, коли в здобутий повідомленні міститься неправдива інформація. При приховуванні признаковой інформації межа між маскуванням і дезінформуванням

розмита. Принципова відмінність між ними полягає в тому, що маскування спрямована на утруднення виявлення об'єкта захисту серед інших об'єктів фону, а дезінформування - на створення помилкового об'єкта прикриття.

Дезінформування відноситься до числа найбільш ефективних методів захисту інформації з наступних причин:

- Створює у власника інформації, що захищається запас часу, обумовлений перевіркою розвідкою достовірності отриманої інформації;

- Наслідки прийнятих конкурентом на основі неправдивої інформації рішень можуть бути для нього гіршими у порівнянні з рішеннями, прийнятими при відсутності видобутої інформації.

Дезінформування здійснюється шляхом підгонки ознак інформаційного портрета, що захищається під ознаки інформаційного портрета помилкового об'єкта, відповідного заздалегідь розробленої версії, - об'єкта прикриття.

5. ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

1. Поняття витоку інформації та технічного каналу витоку інформації.
2. Основні причини та джерела виникнення технічних каналів витоку інформації.
3. Класифікація технічних каналів витоку інформації.
4. Характеристика та можливості оптичних, радіоелектичних, акустичних та матеріально-речових каналів витоку інформації.

5.1 Поняття витоку інформації та технічного каналу витоку інформації

Раніше ми згадували, що будь-яка інформація має свою цінність і вона залежить від доступності інформації і може передаватись шляхом доступу до різноманітних **джерел інформації** (людей, документів, публікацій, технічних носіїв інформації, технічних засобів забезпечення виробничої та трудової діяльності, певної продукції, відходів виробництва та ін.).

В результаті такого доступу виділяють основну мету доступу до інформації:

- ознайомлення – протиправні дії, що не призводять до змін або руйнування інформації;
- модифікація – випадкові або навмисні дії. Що призводять до часткових змін захисту інформації;
- знищення – протиправні дії, що призводять до значного або повного руйнування інформаційних ресурсів.

Окрім того, варто виділити в результаті якого впливу був отриманий доступ до інформації. Зазвичай вплив на джерела інформації поділяють на природній та на штучний, тому загрози класифікують так само:

Природні загрози - це загрози що спричинені діями на систему захисту та її елементи об'єктивних фізичних процесів та стихійних природніх явищ, що не

залежить від людини.

Штучні загрози - це загрози системи захисту, що спричинені діяльністю людини.

Штучні загрози в свою чергу бувають: ненавмисні (викликані помилками в проектуванні системи захисту та її елементів, помилками в програмному забезпеченні, помилками у діях персоналу та ін.) та навмисні (викликані корисливими намаганнями людей - зловмисників).

Результатом загроз зазвичай є несанкціонований доступ до конфіденційної інформації. Зазвичай способи несанкціонованого доступу до інформації класифікують наступним чином:

Розголошення — це навмисні чи необережні дії з конфіденційними відомостями, що призвели до ознайомлення з ними осіб, не допущених до них. Розголошення має вираз в повідомленні, передаванні, представленні, опублікуванні, втраті та в інших формах обміну дії з діловою інформацією.

Витік - це безконтрольний вихід конфіденційної інформації за межі організації чи кола осіб, яким вона була довірена. Витік інформації здійснюється різними технічними каналами.

Канал витоку інформації - це фізичний шлях від джерела конфіденційної інформації до зловмисника, за допомогою якого останній може одержати доступ до відомостей, що охороняються. Канал витоку інформації – потенційні напрями несанкціонованого доступу до інформації, обумовлені архітектурою, технологічними схемами функціонування засобів електронно-обчислювальної техніки, а також невиконанням організаційно-режимних заходів .

5.2 Основні причини та джерела виникнення технічних каналів витоку інформації

Для оперування зі стрімко зростаючим потоком інформації, викликаним науково-технічним прогресом, суб’єкти підприємницької діяльності, установи й організації усіх форм власності змушені постійно поповнювати свій арсенал різноманітними технічними засобами й системами, призначеними для приймання, передачі, обробки і збереження інформації.

Фізичні процеси, що відбуваються в таких пристроях при їхньому функціонуванні, створюють у навколишньому просторі побічні електромагнітні, акустичні та інші випромінювання, що пов’язані з обробкою інформації. Подібні випромінювання можуть виявлятися на досить значних відстанях (до сотень метрів) і, отже, використовуватися зловмисниками, що намагаються одержати доступ до таємної інформації. Тому заходи щодо захисту інформації (ЗІ), яка циркулює в технічних засобах, спрямовані насамперед на зменшення рівнів таких випромінювань.

Побічні електромагнітні випромінювання (ПЕМВ) виникають внаслідок

непередбаченого схемного або конструктивного рішення розглянутого технічного засобу передачі інформації за рахунок паразитних зв'язків за напругою, струмом, зарядом або магнітним полем.

Під паразитним зв'язком розуміють зв'язок по електричних або магнітних колах, що з'являються незалежно від бажання конструктора. У залежності від фізичної природи елементів паразитних електричних кіл розрізняють паразитний зв'язок через загальний повний опір, ємнісний або індуктивний паразитний зв'язок.

У реальних умовах у навколишньому просторі присутні численні завади як природного, так і штучного походження, що істотно впливають на можливі механізми приймання інформації. ТКВІ найчастіше розглядають у сукупності з джерелами завад. Для традиційних систем зв'язку такі завади є негативним явищем, які ускладнюють приймання сигналу, однак для захисту технічних засобів від витоку інформації по побічних каналах ці завади виявляються корисними й нерідко створюються навмисно.

Джерелами випромінювань у технічних каналах є різноманітні технічні засоби, в яких циркулює інформація з обмеженим доступом (ІзОД). Такими засобами можуть бути: • мережі електроживлення і лінії заземлення; • автоматичні мережі телефонного зв'язку; • системи телеграфного, телекодового і факсимільного зв'язку; • засоби гучномовного зв'язку; • засоби звуко- і відеозапису; • системи звукопідсилення мови; • електронно-обчислювальна техніка; • електронні засоби оргтехніки. Одним із джерел випромінювань у ТКВІ може бути і голосовий тракт людини, що викликає появу небезпечних акустичних випромінювань у приміщенні або за його межами. Середовищем поширення акустичних випромінювань у цьому випадку є повітря, а при закритих вікнах і дверях – повітря і довільні звукопровідні комунікації. Якщо при цьому для перехоплення інформації використовується відповідна техніка, то утворюється ТКВІ, який називається акустичним.

Цілком ймовірно припустити, що утворенню ТКВІ сприяють визначені обставини і причини технічного характеру (рис. 5.1).

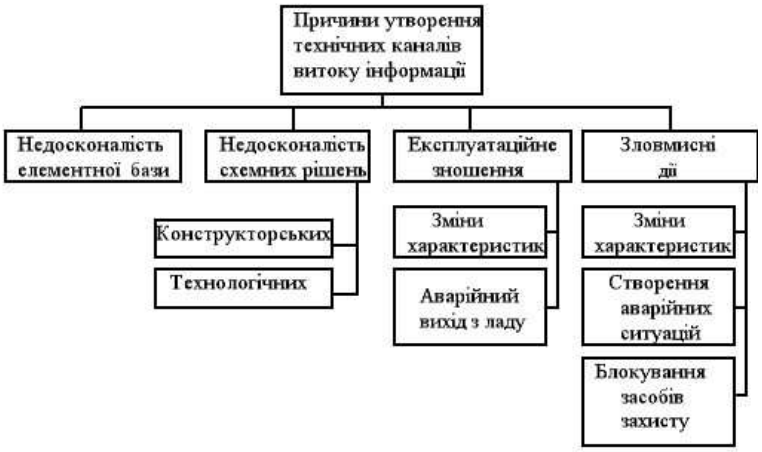

Рисунок 5.1 - Класифікація причин утворення каналів витоку інформації

До них можна віднести недосконаліть елементної бази і схемних рішень, прийнятих для даної категорії технічних засобів, експлуатаційне зношення елементів виробництва, а також злочинні дії.

5.3 Класифікація технічних каналів витоку інформації

Основними джерелами утворення ТКВІ (рис. 5.2) є:

- перетворювачі фізичних величин;
- випромінювачі електромагнітних коливань;
- паразитні зв’язки і наведення на провідники і елементи електронних пристроїв.

У свою чергу, акустичні перетворювачі поділяються на індуктивні, ємнісні, п’єзоелектричні і оптичні. При цьому за видом перетворення вони можуть бути й акустичними, і електромагнітними. Класифікація випромінювачів електромагнітних коливань виконується за діапазоном частот.

Паразитні зв’язки і наведення виявляються у вигляді зворотного зв’язку (найбільш характерний додатний зворотний зв’язок), а втрати – по колах живлення й заземлення.

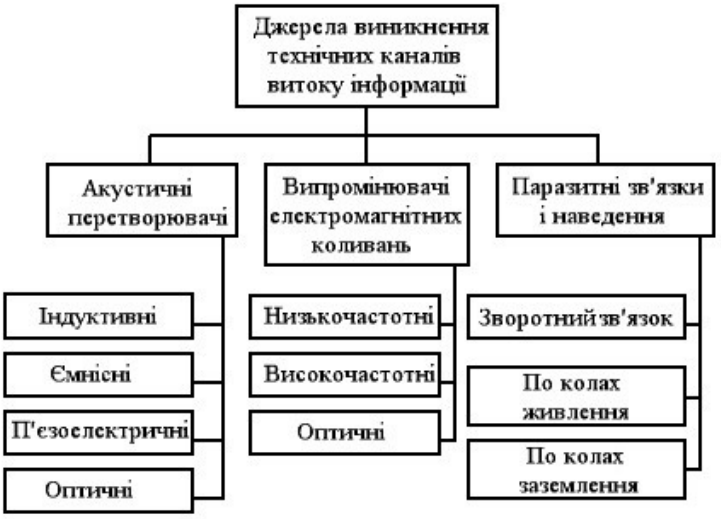

Рисунок 5.2 - Класифікація джерел утворення каналів втрати інформації

Технічні засоби та системи можуть не тільки безпосередньо випромінювати у простір сигнали, що містять інформацію, яка обробляється, але й приймати за рахунок своїх мікрофонних ефектів або антенних властивостей існуючі поблизу акустичні та електромагнітні випромінювання. Технічні засоби можуть перетворювати прийняті випромінювання в електричні сигнали та передавати їх по своїх лініях зв’язку, які, як правило, не контролюються, за територію об’єкта на значні відстані.

Технічні канали витоку інформації прийнято ділити на типи:

- радіоканали (електромагнітні випромінювання радіодіапазона);

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

- електричні канали (небезпечна напруга і струми в різних струмопровідних комунікаціях);

- оптичні канали (електромагнітні випромінювання в інфрачервоній, видимій і ультрафіолетовій частині спектра);

- матеріально-речові канали (папір, фото, магнітні носії, відходи і так далі).

5.4 Характеристика та можливості оптичних, радіоелектичних, акустичних та матеріально-речових каналів витоку інформації

Оптико-електронний канал витоку створюється при опромінюванні лазерним променем вібруючих в акустичному полі тонких відзеркалювальних поверхонь, таких як скло вікон, дзеркал, картин і т.п. Відбите лазерне випромінювання модулюється по амплітуді і фазі та приймається приймачем оптичного випромінювання, при демодуляції якого виділяється мовна інформація. Для перехоплення мовної інформації по даному каналу використовуються локаційні системи, що працюють, як правило, в ближньому інфрачервоному діапазоні і відомі як “лазерні мікрофони”. Дальність перехоплення складає декілька сотень метрів.

Радіоелектронний спосіб витоку інформації — канал, в якому носієм інформації служить електромагнітне поле, електричний струм.

Найбільш інформативним каналом витоку інформації є радіоелектронний канал. Незахищені засоби передачі, прийому й обробки інформації, що працюють від електричного струму утворюють радіоелектронний канал витоку інформації. У радіоелектронному каналі передачі носієм інформації є електричний струм та електричне поле з частотами коливань від звукового діапазону до десятків ГГц.

Матеріально-речовий канал - отримання інформації з відходів виробничої і трудової діяльності. Залежно від профілю роботи підприємства це можуть бути зіпсовані накладні, фрагменти документів, що складаються, чернетки листів, браковані заготовки деталей, панелей, кожухів і інших пристроїв для нових моделей різної техніки, що розробляються підприємством. Особливе місце серед такого роду джерел займають залишки бойової техніки і озброєння на випробувальних полігонах. У рекомендаціях недосвідченому промисловому розвідникові мовиться: “Не гребуйте виступити в ролі сміттяря. Огляд сміттєвих корзин може принести вам багатий улов”.

В **акустичних каналах витоку** інформації середовищем поширення мовних сигналів є повітря. Виток акустичної інформації за межі огороджувальних конструкцій можливий трьома шляхами:

- за рахунок «мембранного ефекту». Так званий «мембранний ефект» обумовлений коливанням тонких (відносно довжини) і, як правило відносно легких, елементів огороджувальних конструкцій (віконного скла, фанерних, гіпсокартонних,

пластикових перегородок тощо), здатних прогинатися під дією звуку;

- через тріщини, отвори, щілини та інші акустичні отвори, тобто прямим розповсюдженням акустичних коливань;
- за рахунок перетворення акустичних коливань в віброакустичні, а потім знов в акустичні. У даному випадку частина енергії акустичних коливань (частина відбивається), падаючи на поверхню огороджувальної конструкції, перетворюється на віброакустичну, тобто в коливання твердих частинок матеріалу без перенесення речовини.

Основними джерелами інформації **матеріально-речового каналу** просочування інформації є:

- чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв.
- відходи діловодства і видавничої діяльності в організації.
- магнітні і інші носії інформації ПЕВМ, на яких під час експлуатації містилася інформація з обмеженим доступом;
- бракована продукція і її елементи;
- відходи виробництва з демаскуючими речовинами в газоподібному, рідкому і твердому вигляді;
- радіоактивні матеріали.

6 ЕЛЕКТРИЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

6.1. Канал побічних електромагнітних випромінювань ОТЗС.

6.2. Канал побічних електромагнітних випромінювань ДТЗС.

6.3. Канал “паразитної” модуляції сигналів ВЧ генераторів.

6.4. Канал “паразитної” ВЧ генерації підсилювачів.

6.5. Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС.

6.6. Канал побічних електромагнітних наведень на комунікації ДТЗС.

6.7. Канал ВЧ нав’язування (для зняття інформації, що обробляється вОТЗС).

6.1.Канал побічних електромагнітних випромінювань ОТЗС

Розглянемо сутність та шляхи (фізичні основи, принципи та порядок) утворення технічних каналів витоку інформації, що обробляється основними технічними засобами та системами. Найнебезпечнішими для витоку інформації, що обробляється в ОТЗС, є канали побічних електромагнітних випромінювань та наведень (канали ПЕМВН).

Канал побічних електромагнітних випромінювань ОТЗС (канал ПЕМВ ОТЗС) утворюється шляхом перехоплення приймачами засобів технічноїрозвідки побічних електромагнітних полів, які формуються навколо електронних елементів та провідників (шлейфів) ОТЗС при проходженні ними інформаційних сигналів та поширення цих полів за межі контрольованої зони. Інформаційними сигналами у

даному випадку є електричні струми, що несуть інформацію.

Навколо ОТЗС, як системи електронних елементів та провідників (шлейфів), в яких відповідно з принципом основної дії ОТЗС циркулюють електричні струми, що несуть інформацію, завжди присутні поля випромінювання. Оскілки ці випромінювання небажані та носять паразитичний (побічний) характер, їх називають побічними електромагнітними випромінюваннями (ПЕМВ). Побічні електромагнітні випромінювання поширюються у вільному просторі і можуть бути перехоплені за межами КЗ приймачами засобів технічної розвідки противника, таким чином утворюється канал ПЕМВ ОТЗС (рис. 6.1).

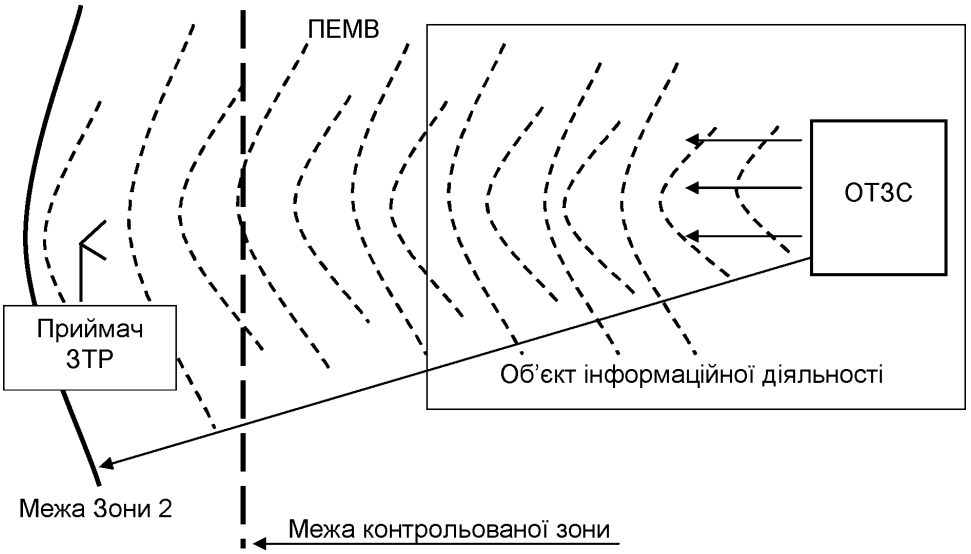

Рисунок 6.1 - Канал побічних електромагнітних випромінювань ОТЗС

При цьому небезпечний сигнал, що несеться цим полем, буде, практично, зруйнований звичайними завадами та шумами. Як вже відмічалося раніше, простір, за межами якого відношення сигналу до завади не перевищує допустиму норму, є Зоною 2 даного ОТЗС.

Розташування приймачів ЗТР противника за межами Зони 2 не дасть можливості перехоплення інформації.

Запобігання витоку інформації каналом ПЕМВ ОТЗС (унеможливлення створення такого ТКВІ) досягається шляхом:

- створення КЗ не меншої за Зону 2 та організації режиму доступу до КЗта на ОІД;
- екранування ОТЗС або локального екранування електронних елементів та провідників (шлейфів) ОТЗС, зменшення довжини провідників (шлейфів) ОТЗС;
- просторового електромагнітного зашумлення на об'єкті ЕОТ.

6.2 Канал побічних електромагнітних випромінювань дтзс

Канал побічних електромагнітних випромінювань ДТЗС, як різновид каналів ПЕМВ, утворюється шляхом перехоплення приймачами засобів технічної розвідки

за межами КЗ небезпечних сигналів у вигляді побічних електромагнітних полів ОТЗС, які перевипромінюються допоміжними технічними засобами та системами, а також сторонніми провідниками (рис. 6.2).

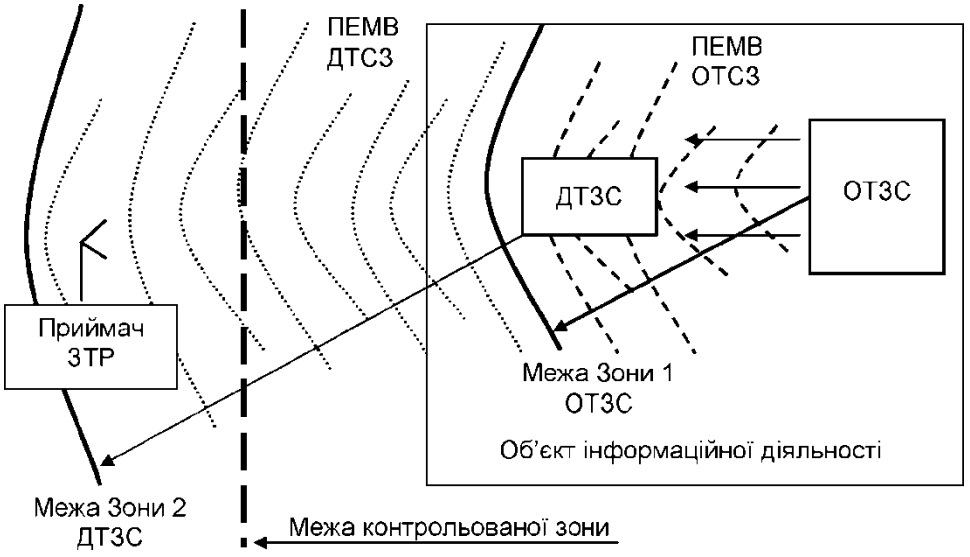

Рисунок 6.2 - Канал побічних електромагнітних випромінювань ДТЗС

Допоміжні технічні засоби та системи, а також сторонні провідники, якщо вони знаходяться в зоні 1 ОТЗС або мають спільні пробіги з лініями, якими поширюються небезпечні сигнали (в тому числі сигнали побічних електромагнітних наведень) ОТЗС, є випадковими антенами і можуть призвести до витоку інформації небезпечними сигналами, наведеними на них побічними електромагнітними випромінюваннями основних технічних засобів та систем.

6.3 Канал "паразитної" модуляції сигналів вч генераторів

Канал "паразитної" модуляції сигналів ВЧ генераторів, як різновид каналів ПЕМВ, утворюється шляхом модуляції небезпечним сигналом високочастотних сигналів ВЧ генераторів ОТЗС, випромінювання модульованих ВЧ коливань у вільний простір та перехоплення таких коливань радіоприймальними пристроями засобів технічної розвідки за межами КЗ (рис. 6.3).

Основні технічні засоби та системи в своєму складі мають генератори високих частот (ВЧ генератори). Практично всі засоби ЕОТ в своєму складі мають генератори тактових частот, гетеродини та інші ВЧ генератори. Високочастотний сигнал ВЧ генератора модулюється низькочастотними небезпечними сигналами, що циркулюють в ОТЗС, та випромінюється у вигляді електромагнітного поля у вільний простір.

Оскільки згасання електромагнітного поля на високих частотах менше ніж на низьких, то поле розповсюджується дальше. А це, в свою чергу, дає можливість перехоплення інформації засобами технічної розвідки за межами Зони 2, розрахованої для сигналу без модуляції.

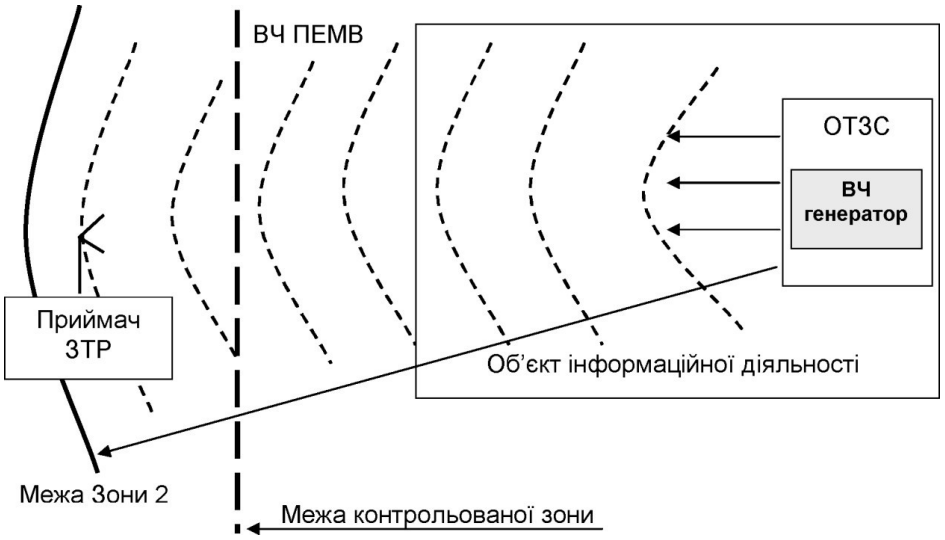

Рисунок 6.3 - Канал "паразитної" модуляції сигналів ВЧ генераторів

Слід відмітити, що модуляція розширює спектр частот сигналу, підвищує його потужність і завадостійкість. Тому Зона 2 має розраховуватись з врахуванням модульованого випромінювання на частотах ВЧгенераторів ОТЗС.

6.4 Канал "паразитної" вч генерації підсилювачів

Канал "паразитної" ВЧ генерації підсилювачів, як різновид каналів ПЕМВ, утворюється шляхом самозбудження підсилювачів низької частоти (НЧ) ОТЗС на гармоніках, кратних небезпечному сигналу, поширення їх у вигляді поля електромагнітного випромінювання за межі КЗ та перехоплення цього поля радіоприймальними пристроями засобів технічної розвідки (рис. 6.4).

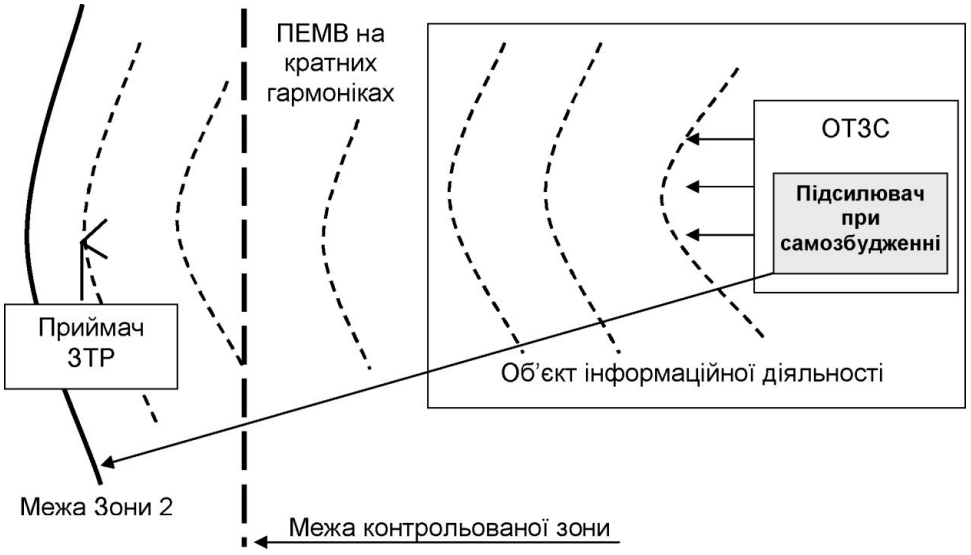

Рисунок 6.4 - Канал "паразитної" ВЧ генерації підсилювачів

У результаті старіння чи інших причин параметри електронних елементів та характеристики негативного зворотного зв'язку можуть змінитись і призвести до порушення режиму роботи самого підсилювача вцілому. Негативний зворотній

зв'язок може змінюватися в бік позитивного, коефіцієнт підсилення збільшується і, разом з цим, зростає нелінійність підсилення, підсилювальний елемент переходить в режим насичення.

Зворотній зв’язок на деяких частотах стає позитивним, і підсилювач перетворюється в генератор. При цьому в режимі насичення кратні гармоніки сигналу можуть суттєво зростати, а їх поле електромагнітного випромінювання може досягти значного рівня. А це, в свою чергу, може дати можливість перехоплення інформації засобами технічної розвідки за межами Зони 2, розрахованої без врахування “паразитної” генерації.

Ефект “паразитної” генерації характеризується нерегулярністю появи, тому одним із способів запобігання витоку інформації таким каналом є своєчасне виявлення (індикація) сигналів “паразитної” генерації та блокування роботи ОТЗС.

6.5 Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) отзс

Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС, як різновид каналів побічних електромагнітних наведень (каналів ПЕМН), утворюється шляхом безпосереднього зняття з ліній електроживлення (заземлення) ОТЗС засобами технічної розвідки за межами КЗ небезпечних електричних сигналів, що наводяться в цих лініях побічними електромагнітними полями ОТЗС та/або просочуються (стікають) в ці лінії (або виникають в лінії електроживлення через нерівномірність споживання електроенергії) при функціонуванні ОТЗС (рис. 6.5).

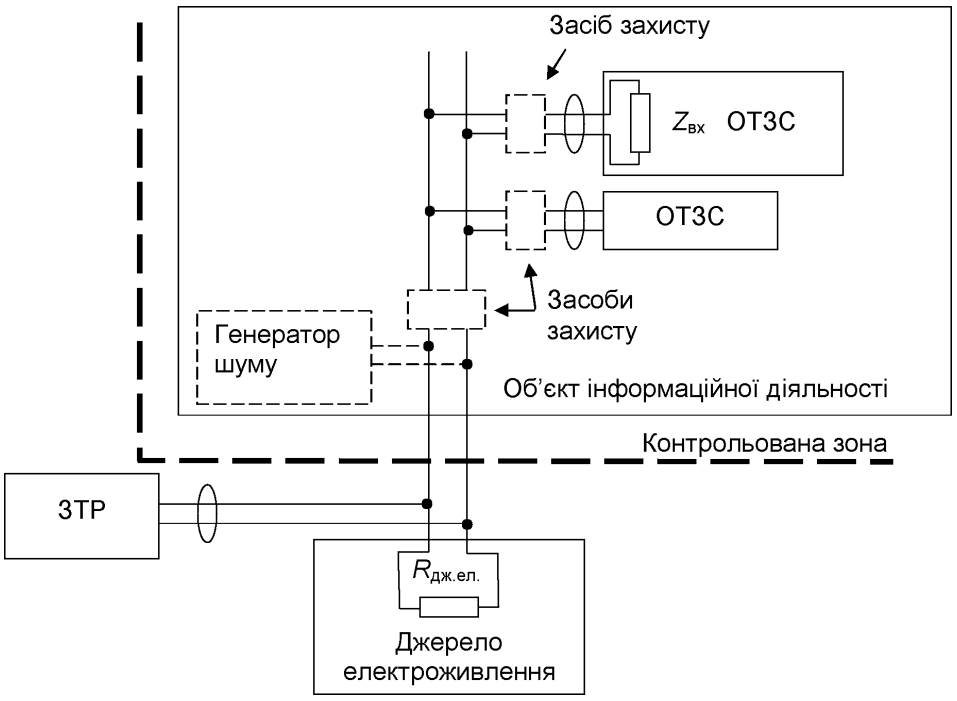

Рисунок 6.5 - Канал побічних електромагнітних наведень на лінії електроживлення ОТЗС

Практично всі технічні засоби та системи обробки та передачі інформації живляться електричною енергією. Лінії електроживлення (заземлення) даних ОТЗС знаходяться в Зоні 1 ОТЗС, тому на них може наводитися за принципом електромагнітної індукції електричний струм, який змінюється аналогічно небезпечному електромагнітному сигналу, і поширюється лініями електроживлення (заземлення).

Також під час обробки інформації вхідний опір ОТЗС може змінюватись за законом сигналів, що обробляються в них. Так, наприклад, підсилювачі (ключові схеми) працюють так, що вхідний (управляючий) сигнал управляє в схемі опором напівпровідника, який формує від джерела живлення підсилений сигнал.

В результаті коливання вхідного опору ОТЗС в ланцюгу електроживлення з'явиться змінна складова небезпечного сигналу по струму, яка на власному опорі джерела електроживлення створюватиме змінну складову напруги. Остання може стати доступною всім абонентам цієї мережі електроживлення, а якщо джерело електроживлення знаходиться за межами КЗ (лінії електроживлення виходять за межи КЗ), то противник може зняти інформацію шляхом безпосереднього підключення засобів технічної розвідки до лінії електроживлення.

Для забезпечення безпеки життєдіяльності персоналу всі технічні засоби заземлюються. Сутність заземлення полягає у тому, що корпус технічного засобу гальванічно зв'язується з ґрунтом "Землі" і потенціал, який накопився на корпусі, ланцюгами заземлення стікає в ґрунт, приймаючи його нульовий потенціал. Якщо система заземлення надійна і опір її досить малий, то стікання буде проходити швидше і корпус технічного засобу обробки інформації практично постійно буде нейтрально зарядженим. Однак на практиці система заземлення не завжди може мати потрібний опір і противник може цим скористатися. Технічний канал витоку інформації ланцюгами заземлення ОТЗС наведений на рис. 6.6.

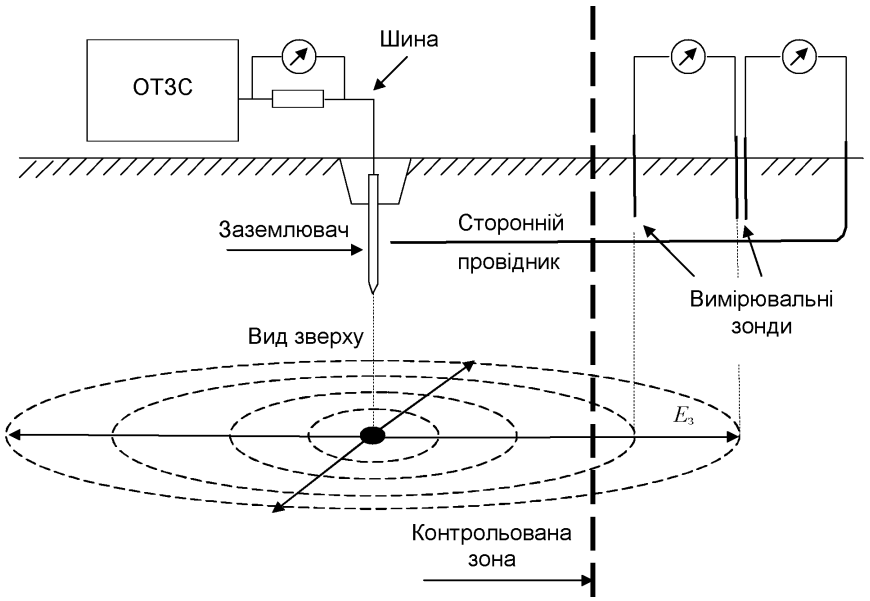

Рисунок 6.6 - Технічний канал витоку інформації ланцюгами заземлення ОТЗС

6.6 Канал побічних електромагнітних наведень на комунікації ДТЗС

Канали побічних електромагнітних наведень на комунікації ДТЗС, як різновид каналів ПЕМН, утворюється шляхом безпосереднього зняття з комунікацій ДТЗС (ліній електроживлення, заземлення та передачі даних ДТЗС, ліній зв'язку, ліній охоронних, протипожежних чи загальних систем безпеки, систем енергопостачання та інших систем) небезпечних електричних сигналів, що наводяться в цих комунікаціях побічними електромагнітними полями ОТЗС, полями комунікацій ОТЗС при їх спільному пробігу з комунікаціями ДТЗС (рис. 6.7).

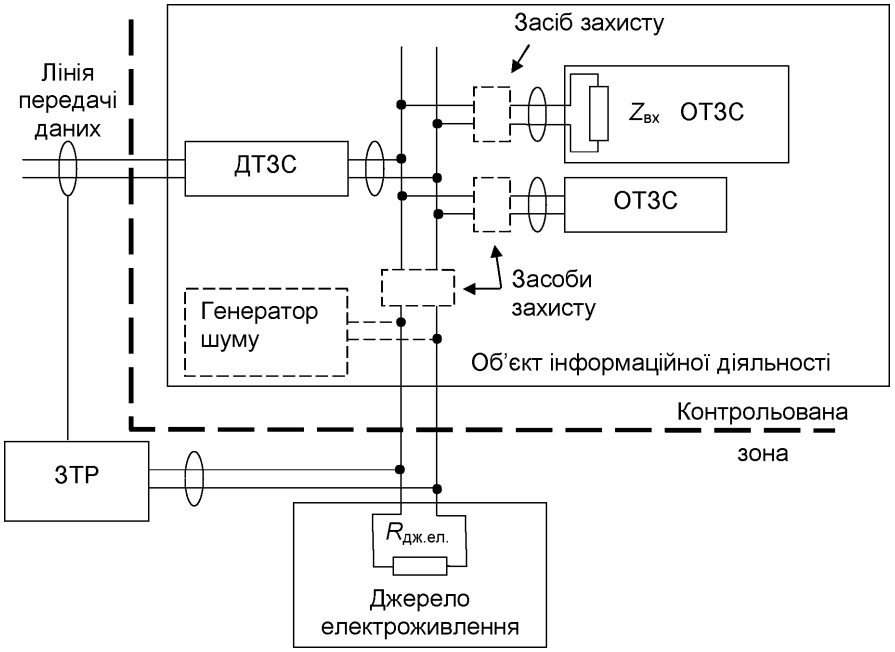

Рисунок 6.7 - Канали ПЕМН на комунікації ДТЗС

6.7 Канал ВЧ нав'язування (для зняття інформації, що обробляється в ОТЗС)

Канал ВЧ нав'язування (для зняття інформації, що обробляється технічними засобами), як різновид параметричних каналів, утворюється шляхом введення ("нав'язування") спеціально створеного високочастотного сигналу (ВЧ-сигналу) в основні та/або допоміжні технічні засоби та системи їх комунікаціями з-за меж контрольованої зони, модуляції цього ВЧ-сигналу небезпечним сигналом на нелінійних елементах ОТЗС та/або ДТЗС та або відбиття цього ВЧ-сигналу від неузгоджених навантажень в ОТЗС та/або ДТЗС, поширення такого модульованого ВЧ- сигналу комунікаціями ОТЗС та/або ДТЗС за межі КЗ та його зняття засобами технічної розвідки при безпосередньому їх підключенні до комунікацій ОТЗС та/або ДТЗС за межами КЗ; або випромінювання такого модульованого ВЧ-сигналу у вільний простір та перехоплення такого випромінювання радіоприймальними засобами технічної розвідки за межами КЗ (рис. 6.8).

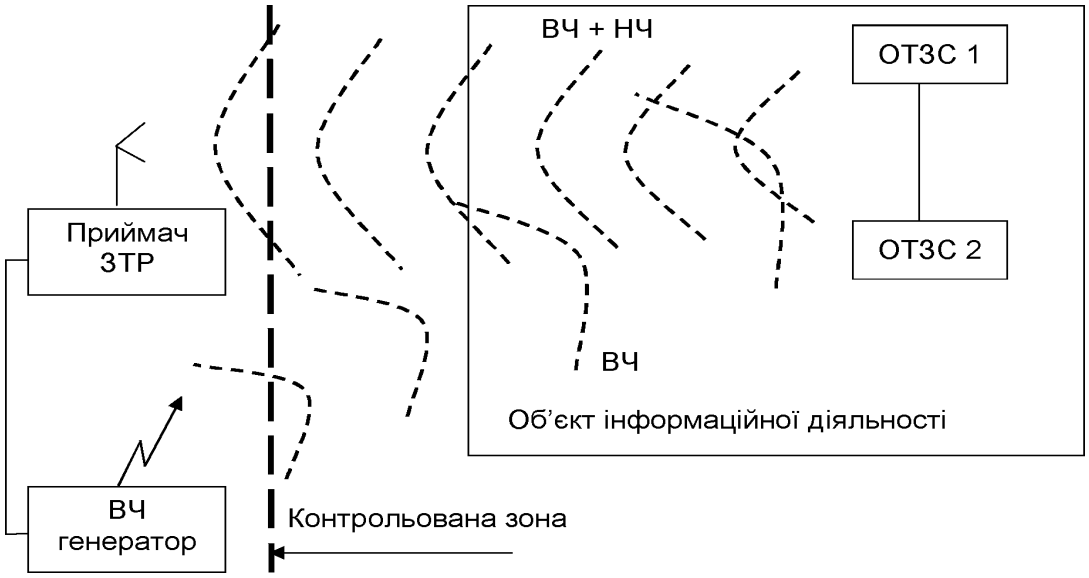

Рисунок 6.8 - Канал ВЧ нав'язування (для зняття інформації, що обробляється в ОТЗС)

Майже всі технічні засоби обробки інформації використовують напівпровідникові електронні елементи, провідність (опір) яких залежить від різниці потенціалів на їх полюсах. Якщо опромінити технічні засоби обробки інформації електромагнітним полем високої частоти (в мегагерцовому діапазоні), то в його ланцюгах, де циркулює небезпечний сигнал, з'являться наведені ВЧ струми, які, в свою чергу, впливатимуть на опори напівпровідниківта інші параметри схем ТЗС. В результаті в схемах здійсниться паразитна модуляція небезпечного сигналу з переносом його спектру ВЧ область. Перевипромінювання такого модульованого ВЧ сигналу може спричинити витік інформації.

Слід відмітити, що при цьому досить просто реалізувати перехоплення такого модульованого ВЧ сигналу, використавши когерентний прийомом, який забезпечує максимум завадостійкості.

Таким чином розглянуті основні різновиди технічних каналів витоку інформації, які утворюються при її обробці в ОТЗС та основні заходи щодо запобігання витоку інформації цими каналами (унеможливлення створення таких ТКВІ).

7 РАДІОЕЛЕКТРОННІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

7.1 Радіоелектронний канал.
7.2 Структура радіоелектронного каналу витоку інформації.
7.3 Види витоку інформації.
7.4 Провідні лінії зв'язку.
7.5 Лінії радіозв'язку і радіорелейні лінії.
7.6 Класифікація перешкод.

7.1 Радіоелектронний канал

В радіоелектронному каналі передачі носієм інформації є електричний струм та електромагнітне поле із частотами коливань від звукового діапазону до десятків ГГц. Радіоелектронний канал відноситься до найбільш інформативних каналів витоку в силу наступних його особливостей:

- незалежність функціонування каналу від часу доби і пори року, істотно менша залежність його параметрів у порівнянні з іншими каналами від метеоумов;
- висока достовірність видобутку інформації, особливо при перехопленні її в функціональних каналах зв'язку (за винятком випадків дезінформації);
- великий обсяг видобутої інформації;
- оперативність отримання інформації аж до режиму реального часу;
- скритність перехоплення сигналів та радіо-теплові спостереження.

Причинами утворення радіоканалів витоку інформації, є наступні фактори:

- недосконаліть елементної бази технічних об'єктів; недосконаліть схемних рішень та проектування виробів;
- експлуатаційний знос і старіння об'єктів РМ; злочинні дії (створення проблемної ситуації, блокування засобів
- захисту, зміна характеристик об'єктів). Утворенню каналів РМ повинні сприяти визначені просторово-
- почасові й енергетичні умови, а також відповідні засоби сприйняття і фіксації інформації, як з боку зловмисника, так і з позиції можливого РМ.

Стосовно до існуючої практики прояву відзначених умов. визначальну фізичну природу утворення каналів витоку інформації, можна вказати на наступні їхні класифікаційні групи: електромагнітні; акустичні; візуально-оптичні та паразитні зв’язки та наведення (рис. 7.1).

Рисунок 7.1 - Радіоканали витоку інформації

В радіоелектронному каналі використовується перехоплення радіо і електричних сигналів, радіолокаційне та радіо-теплове спостереження. В рамках цього з каналу витоку видобувається семантична інформація, видові і сигнальні демаскуючі ознаки. Радіоелектронні канали витоку інформації використовують радіо, радіотехнічна, радіолокаційна і радіо-теплова розвідка.

7.2 Структура радіоелектронного каналу витоку інформації

Структура радіоелектронного каналу витоку інформації в загальному випадку включає (рис. 7.2) джерело сигналу або передавач, середовище поширення електричного струму або електромагнітної хвилі і приймач сигналу.

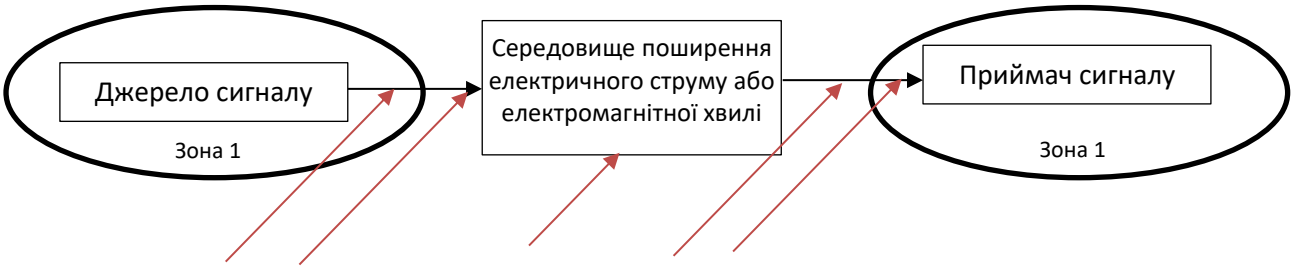

Рисунок 7.2 - Структура радіоелектронного каналу просочування інформації

В радіоелектронних каналах витоку інформації джерела сигналів можуть бути чотирьох видів:

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

Середовищем поширення радіоелектронного каналу витоку інформації є атмосфера, безповітряний простір і направляючі - електричні дроти різних типів та хвилеводи.

Хвилевід — структура, призначена для передачі хвиль, електромагнітних, звукових, або іншої природи, в якій хвиля обмежена в одному чи двох вимірах повним внутрішнім відбиттям на межі.

Інформаційне повідомлення у вигляді електричного струму поширюється по дротах, а електромагнітне поле - в атмосфері, в безповітряному просторі або по напрямних хвилеводів. У приймачі відбувається виділення (селекція) носія з інформацією, що цікавить одержувача по частоті, посилення виділеного слабкого сигналу та зчитування з нього інформації - **демодуляція**.

7.3 Види витоку інформації

Внаслідок наявності визначених форм утворення радіоканалів витоку інформації (рис.7.3) зловмисник знаходить адекватні способи її перехоплення.

Найбільш поширеним в практиці промислового шпигунства знайшли способи негласного знімання інформації:

- підслуховування розмов у приміщенні або автомашині за допомогою радіотехнічних засобів знімання інформації (РЗЗІ);
- контроль провідних телефонних і факсимільних ліній зв'язку з використанням РЗЗІ;
- контроль радіотелефонів, систем персонального виклику і радіостанцій використанням засобів РМ;
- знімання інформації з технічних засобів обробки та збереження за допомогою РЗЗІ;
- дистанційне перехоплення з використанням засобів РМ інформативних побічних випромінювань технічних засобів, експлуатованих на об'єкті;
- знімання акустичної інформації (мікрофонний ефект).

Для реалізації зазначених способів несанкціонованого доступу до каналів витоку інформації зловмисник повинний скористатися адекватними засобами її зняття. Приведені засоби несанкціонованого знімання інформації диференціюються по ряду ознак на більш дрібні підгрупи, що відрізняються специфікою використання конкретних технічних засобів (рис. 7.3).

Рисунок 7.3 - Класифікація можливих засобів зняття інформації з радіотехнічних каналів

В залежності від способу перехоплення інформації розрізняють два види радіоелектронного каналу просочування інформації. У каналі витоку 1-го виду проводиться перехоплення інформації, переданої по функціональному каналу

зв'язку. З цією метою приймач сигналу каналу витоку інформації налаштовується на параметри сигналу функціонального радіоканалу або підключається (контактно чи дистанційно) до дротів відповідного функціонального каналу.

7.4 Провідні лінії зв'язку

Розглянувши канали витоку інформації, слід зазначити, що поняття “канал витоку інформації” стосується до логічного рівня. Дійсно, канал витоку інформації існує не сам по собі, а завдяки наявності певних об’єктів і технічних засобів, що взаємодіють між собою. Сукупність призначених для передачі інформації на відстань технічних засобів і передавального середовища називається каналом зв’язку. Передавальні середовища називаються лініями зв’язку (провідна, радіо і т.ін.).

За призначенням канали зв’язку поділяються на телефонні, телеграфні, телевізійні та ін. За характером експлуатації – на виділені й комутовані. Виділеними (абонентськими) каналами зв’язку називаються канали, які постійно ввімкнені між двома пунктами. Комутовані канали вмикаються тільки за запитом і від’єднуються автоматично після завершення сеансу зв’язку.

Залежно від характеру коливань, які використовуються для передачі інформації, канали називаються електричними, електромагнітними, оптичними, акустичними, пневматичними і т.ін.

Лінії зв’язку поділяються на:

- основні (використовуються для передачі секретних відомостей);
- допоміжні (використовуються для передачі інформації, що не є секретною).

Крім того, лінії зв’язку позначаються номерами, що відповідають режиму інформації, яка передається:

- лінія №1 (лінія передачі секретної інформації);
- лінія №2 (внутрішня телефонна мережа);
- лінія №3 (зовнішня телефонна мережа).

Лінії зв’язку за характеристиками передавального середовища можна поділити на провідні лінії, високочастотні лінії, повітряні лінії електропередачі високої напруги, лінії радіозв’язку і радіорелейні лінії, лінії розподільних силових мереж.

Способи та засоби передачі електричних сигналів по дротах розглядаються у прикладній області радіотехніки, яку ще називають **провідним зв'язком**.

Провідні лінії (повітряні і кабельні) характеризуються первинними (погонні, активний послідовний опір, ємність, індуктивність і провідність) і вторинними (згасання, хвильовий опір і пропускна здатність) параметрами.

Високочастотні лінії зв’язку застосовуються у високочастотних каналах. Останні є сукупністю спеціальної передавальної, ретрансляції і приймальної

апаратури і ліній зв’язку, призначених для незалежної від інших каналів передачі повідомлень на відстань струмами високої частоти. Частотне ущільнення струмами високої частоти дозволяє утворити на основі однієї провідної лінії кілька додаткових каналів зв’язку. Такі канали широко застосовуються при передачі інформації телефонного, телеграфного та іншого зв’язку повітряними сталевими, мідними і біметалічними колами або симетричними і коаксіальними кабелями зв’язку.

Повітряні лінії електропередачі високої напруги широко застосовуються як для зв’язку, так і для передачі телеметричних повідомлень. Останніми роками вони починають застосовуватися для телеконтролю й телекерування місцевими електростанціями, підстанціями та іншими установками в сільському господарстві, а також як резервні лінії зв’язку загальнодержавного значення.

Лінії електропередачі 35, 110, 220 і 400 кВ мають високу електричну й механічну міцність, тому канали зв’язку на їх основі характеризуються високою надійністю (за умови, звичайно, що каналоутворююча апаратура також володіє високою надійністю).

Ці канали мають порівняно високий рівень завад, тому для досягнення достатнього для нормальної роботи відношення сигнал/завада застосовується спеціальна апаратура каналів із порівняно високою вихідною потужністю сигналу, а також якісні фільтри для розділення сигналів і зменшення перехресних завад.

7.5 Лінії радіозв’язку і радіорелейні лінії

Характерною особливістю ліній радіозв’язку є можливість значної дії завад від сусідніх радіостанцій і промислових джерел радіоперешкод порівняно із провідними лініями. До цього виду ліній належать космічна, радіорелейна, КХ, УКХ, мобільний і стільниковий зв’язки.

Лінії розподільних силових мереж широко використовуються для створення каналів циркулярної передачі команд масовим об’єктам як у ряді європейських країн (Франція, Австрія та ін.), так і на території колишнього СРСР. За допомогою таких каналів здійснюється централізоване ввімкнення вуличного освітлення, передача пожежної тривоги, команд цивільної оборони і т.ін.

Команди (сигнали) передаються лише в одному напрямі з центрального пункту, а у відповідь попереджувальна сигналізація відсутня.

Різновидом розподільних силових мереж є контактні мережі для електричного транспорту. Вони використовуються як канали телефонного зв’язку з рухомим складом і для передачі повідомлень телекерування, телесигналізації і телевимірювання.

З усіх перерахованих ліній зв’язку можна здійснити зняття інформації, використовуючи для цього наступні методи:

- гальванічне під’єднання до лінії;
- електромагнітний метод;
- індукційне зняття за допомогою кліщів.

Повітряні лінії зв'язку відносяться до симетричних ланцюгів, відмітною особливістю яких є наявність двох провідників з однаковими електричними властивостями. В залежності від типу несучих конструкцій вони діляться на стовпові і стоечні. Стовповою називаються лінії, несучими конструкціями є дерев'яні або залізобетонні опори. Опорами стовпових ліній служать металеві стійки, встановлені, наприклад, на дахах будівель. Для ізоляції проводів повітряних ліній один від одного і щодо землі їх зміцнюють порцеляновими ізоляторами. Більш широко застосовуються кабельні лінії зв'язку. Кабельні лінії зв'язку отримали домінуючий розвиток на ринку при організації зв'язку на об'єктах та міських чи міжміських лініях телефонного зв'язку. Вони становлять приблизно 65% телефонних ліній в країні. Кабелі бувають симетричними та коаксіальними.

Симетричний кабель - це кабель, що складається в основному з двох або більше пар скручених разом провідників, кожний з яких відзначається однаковою конструкцією (діаметром, ізоляцією). Всередині С. к. є й інші пари провідників. Провідником у С. к. служить головним чином мідь, ізоляційним матеріалом — пластмаса чи папір.

Коаксіáльний ка́бель (від англ. coaxial — співвісний) — електричний кабель із співвісними провідниками. Сучасний кабель складається з центрального провідника, оточеного шаром діелектрика, зовнішня поверхня якого покрита обплетенням або фольгою (другим провідником) і захисною оболонкою з пластику, що захищає кабель від дії навколишнього середовища.

За частотою електромагнітні хвилі класифікуються відповідно до Регламенту радіозв'язку, затвердженим на Всесвітній адміністративної конференції в Женеві в 1979 р. (табл. 7.1).

Таблиця 7.1 – Характеристики електромагнітних хвиль

Діапазон довжин хвиль	Найменування хвиль	Позначення і найменування частот	Діапазон частот
> 100 км	-	ELF-надзвичайно низькі	Частки Гц-3 кГц
10 - 100 км	Міріаметровиє	VLF (ОНЧ)-дуже низькі	3-30 кГц
1 - 10 км	Кілометрові (Довгі)	LF (НЧ)-низькі	30-300 кГц
100 - 1000 м	Гектаметровие (Середні)	MF (СЧ)-середні	300-3000 кГц
10 - 100 м	Декаметрових (Короткі)	HF (ВЧ)-високі	3-30 МГц
1 - 10 м	Метрові	(ДВЧ)-дуже високі	30-300 МГц
10 - 100 см	Дециметрові	UHF (УВЧ)-ультрависокі	300-3000 МГц
1 - 10 см	Сантиметрові	SHF (НВЧ)-надвисокі	3-30 ГГц
1 - 10 мм	Міліметрові	EHF (КВЧ)-вкрай високі	30-300 ГГц
0.1- 1 мм	Децимілiметрові	ГВЧ-гіпервисокіе	300-3000 ГГц

Потужність випромінювання електромагнітного поля тим вище, чим ближче частота коливань у розподіленому контурі, утвореного індуктивністю провідників і розподіленої ємністю між ними і землею, до частоти сигналу. Пристрої, в яких забезпечується ефективне перетворення енергії електричних сигналів в електромагнітну хвилю, називаються **антенами**.

Антенні пристрої є невід'ємною частиною передавальних і прийомних радіоелектронних засобів. Причому їх конструкція залишається незмінними в режимах передачі і прийому, за винятком тих випадках, коли випромінюється велика потужність. У цьому випадку доводиться приймати додаткові заходи щодо запобігання електричного пробою в високовольтних ланцюгах передавальної антени, необхідність у яких відсутній для приймальні. У загальному випадку принцип оборотності дозволяє передавальну антену використовувати в якості прийомної і навпаки.

Характер поляризації електромагнітної хвилі залежить від конструкції та розташування випромінюючих елементів антени. Невідповідність поляризації електромагнітної хвилі просторової орієнтації елементів прийомної антени, в яких наводяться електричні заряди, призводить до зменшення величини цих зарядів. Радіохвилі в залежності від умов розповсюдження діляться на земні (поверхневі), прямі, тропосферні й іоносферні (просторові).

Земними називаються радіохвилі, які поширюються в безпосередній близькості від поверхні Землі і частково огинають її поверхню завдяки явищу дифракції. **Прямими** названі радіохвилі, що розповсюджуються прямолінійно в атмосфері та космосі.

Радіохвилі, які поширюються в **тропосфері** - приземної неоднорідною області атмосфери не вище 10 - 12 км від поверхні Землі, називаються тропосферних. У тропосфері відбувається розсіювання, а також часткове викривлення траєкторії і відбиття радіохвиль від неоднорідностей тропосфери.

Іоносферними називають радіохвилі, що розповсюджуються в результаті послідовного відображення від іоносфери і земної поверхні. Іоносферу утворюють іонізовані під дією ультрафіолетового випромінювання Сонця верхні шари атмосфери. Концентрація вільних електронів в іоносфері змінюється по висоті.

У іоносфері відбувається заломлення, відображення і поглинання радіохвиль. **Заломлення** радіохвиль обумовлено змінами діелектричної проникності, а, отже, показника заломлення по висоті шарів. У міру поширення радіохвиль від наземного джерела через більш високо розташовані шари показник заломлення зменшується, траєкторія електромагнітної хвилі викривляється і за певних умов хвиля повертається на Землю.

Відображення радіохвиль на тій чи іншій висоті іоносфери залежить від частоти радіохвиль і кута їх падіння на шар. За інших рівних умов чим більше кут падіння хвилі, відлічуваний від вертикальної лінії в точці падіння, тим більше

пологу траєкторія променю в іоносфері і тим менша електронна концентрація буде потрібно для повернення променю на Землю. Мінімальне значення кута падіння, при якому ще можливо відбиття радіохвиль від іоносфери називається критичним. При куті падіння, меншому критичного, радіохвилі проходять через іоносферу не позначившись.

Так як коефіцієнт заломлення зменшується зі збільшенням частоти, то довгі хвилі заломлюються сильніше, ніж короткі, а для УКХ переломлення недостатньо для повернення хвиль на Землю і вони йдуть в космічний простір. Найвища частота, при якій електромагнітна хвиля ще може повернутися на Землю, називається максимально застосовної частотою. Але значення цієї частоти неоднозначно внаслідок залежності її від кута падіння. Тому вводять поняття **критичної частоти**, яка є максимально застосовної частотою при куті падіння 90 градусів. З визначення випливає, що ця частота є нижчу з усіх максимально застосовних частот.

За рахунок багаторазового відбиття радіохвиль від шарів іоносфери і земної поверхні електромагнітна хвиля може поширюватися на великі відстані. Але при відбитті виникають зони мовчання, куди не потрапляють відбиті від іоносфери електромагнітні промені. У зонах прийому відбувається інтерференція хвиль, що пройшли різний шлях від випромінювача і мають, отже, різні фази. Випадковий характер зміни фаз приводить до випадкового зміни амплітуди результуючої хвилі, яке називається завмиранням або федингом.

Ступінь **поглинання** радіохвиль в атмосфері збільшується при підвищенні щільності іонізації, частоти коливання та шляхи, яку проходить радіохвилею в іоносфері. Взимку, коли концентрація електронів у зв'язку з пониженням сонячної радіації зменшується, поглинання радіохвиль знижується і дальність розповсюдження збільшується.

Радіохвилі у діапазоні ультракоротких (метрових) і більш коротких хвиль є основними носіями інформації в мережах телекомунікацій людства в силу таких особливостей:

- Мають величезний частотний діапазон, що забезпечує можливість передачі величезного обсягу інформації, в тому числі шляхом використання широкосмугових каналів;
- Низький рівень атмосферних і промислових перешкод, що дозволяють використовувати приймальні пристрої з високою чутливістю, що підвищує дальність прийому;
- Слабкий вплив станційних перешкод на роботу інших радіосистем внаслідок обмеженості їх радіусу видимості;
- Можливість створення невеликих антен з вузькою діаграмою спрямованості, що дозволяють здійснювати радіозв'язок при відносно малій потужності передавальних пристроїв.

Основним недоліком радіохвиль розглянутого діапазону - мала дальність розповсюдження і суттєво більшу поглинання їх природними опадами (дощем, туманом, снігом, градом), особливо в міліметровому і коротших діапазонах.

7.6 Класифікація перешкод

При розповсюдженні радіохвиль в місті характер їх поширення істотно спотворюється порівняно з поширенням на відкритих просторах за рахунок численних перевідбиттів від стін будівель і приміщень і загасання в них. Ці обставини необхідно враховувати при оцінці просторової орієнтації і можливостей каналів витоку інформації.

Екранувальні властивості деяких елементів будинку наведені в табл. 7.2.

Зазначені в таблиці дані отримані для стін, 30 відсотків площі яких займають віконні прорізи зі звичайним склом. Якщо віконні прорізи закриті металевими гратами з вічком 5 см , То екранування збільшується на 30-40%. Дальність розповсюдження електромагнітної хвилі з будівлі із товстої цегляної або залізобетонної стінами зменшується по відношенню до екранованих стін дерев'яного будинку в 2-3 рази залежно від частотного діапазону.

Таблиця 7.2 - Екранувальні властивості елементів будинку

Тип будівлі	Ослаблення, дБ на частоті		
	100 МГц	500 МГц	1 ГГц
Дерев'яне будинок з товщиною стін 20 см	5-7	7-9	9-11
Цегляна будівля з товщиною стін 1.5 цегли	13-15	5-17	16-19
Залізобетонне будівлю з осередком арматури 15х15 см і товщиною 160 мм	20-25	18-19	15-17

Різноманіття природних і штучних джерел випромінювань в радіодіапазоні породжує проблему електромагнітної сумісності носія інформації з іншими випромінюваннями-носіями іншої інформації, які являють собою перешкоди стосовно розглянутого радіосигналу (рис. 7.4).

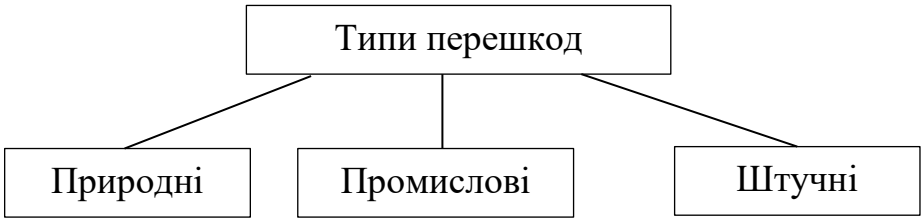

Рисунок 7.4 - Класифікацію перешкод у каналах витоку

Природні перешкоди викликаються наступними природними явищами:

- Електричними грозовими розрядами на частотах менше 30 МГц.
- Переміщенням електрично заряджених часток хмар, дощу, снігу та ін.
- Виникненням резонансних електричних коливань між землею та іоносферою.
- Тепловим випромінюванням Землі та будівель в діапазоні більше 30-40 МГц.
- Сонячною активністю в основному на частотах більше 20 МГц.
- Електромагнітними випромінюваннями неба, Місяця, інших планет (на частотах понад 1 МГц).
- Тепловими шумами в елементах радіоприймачах.

У містах до природних перешкод додаються промислові перешкоди, які за характером спектра випромінювань поділяються на флуктуаційні, гармонійні і імпульсні. Флуктуаційні перешкоди мають розподілений по частоті спектр і створюються коронами високовольтних електропередач, лампами денного світла, неоновою рекламою, електрозварюванням та іншими електричними процесами.

Маскуючі перешкоди створюють фонові перешкоди, завдяки яким ускладняється або виключається виявлення і розпізнавання корисних сигналів.

Імітують перешкоди за структурою близькі до корисних сигналів які при прийомі можуть ввести в оману одержувача. За співвідношенням спектру перешкод і корисних сигналів перешкоди підрозділяються на загороджувальні і прицільні. Загороджувальні перешкоди мають ширину спектру частот, що значно перевищує ширину спектру корисного сигналу, що дозволяє пригнічувати сигнал без точного налаштування на його частоту.

По тимчасовій структурі випромінювання перешкоди бувають неперервні та імпульсні (у вигляді немодульований або модульованих радіоімпульсів).

8. АКУСТИЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

8.1. Технічний канал витоку інформації.
8.2. Типи сигналів та шляхи їх витоку.
8.3. Віброакустичні канали.
8.4. Акустоелектричні канали.
8.5. Оптико - електронний (лазерний) канал.
8.6. Параметричні канали.

8.1 Технічний канал витоку інформації

Під технічним каналом витоку інформації (ТКВІ) розуміють сукупність об'єкта розвідки, технічного засобу розвідки (ТЗР), за допомогою якого добувається інформація про цей об'єкт, і фізичного середовища, у якій поширюється інформаційний сигнал. По суті, під ТКВІ розуміють спосіб одержання за допомогою ТЗР розвідувальної інформації про об'єкт.

Сигнали є матеріальними носіями інформації. По своїй фізичній природі

сигнали можуть бути електричними, електромагнітними, акустичними і т.д. Тобто сигналами, як правило, є електромагнітні, механічні і інші види коливань (хвиль), причому інформація втримується в їхніх параметрах, що змінюються.

Залежно від природи сигнали поширюються в певних фізичних середовищах. У загальному випадку середовищем поширення можуть бути газові (повітряні), рідинні (водні) і тверді середовища, Наприклад, повітряний простір, конструкції будинків, сполучні лінії і струмопровідні елементи, ґрунт(земля) і т.п.

Технічні засоби розвідки служать для прийому і виміру параметрів сигналів. Під акустичною розуміється інформація, носієм якої є акустичні сигнали. У тому випадку, якщо джерелом інформації є людська мова, акустична інформація називається **мовною**. Акустичний сигнал являє собою збурювання пружного середовища, що проявляються у виникненні акустичних коливань різної форми і тривалості. Акустичними називаються механічні коливання часток пружного середовища, що поширюються від джерела коливань у навколишній простір у вигляді хвиль різної довжини.

Первинними джерелами акустичних коливань є механічні коливальні системи, наприклад органи мови людини, а вторинними - перетворювачі різного типу, у тому числі електроакустичні. Останні являють собою пристрої, призначені для перетворення акустичних коливань в електричні і назад. До них ставляться п’єзоелементи, мікрофони, телефони, гучномовці і інші пристрої.

8.2 Типи сигналів та шляхи їх витоку

Залежно від форми акустичних коливань розрізняють прості і складні сигнали. Тональний - це сигнал, викликаний коливаннями, що відбуваються за синусоїдальним законом. Складний сигнал включає цілий спектр гармонійних складових. Мовний сигнал є складним акустичним сигналом у діапазоні частот від 200...300 Гц до 4…6 кГц. Залежно від фізичної природи виникнення інформаційних сигналів, середовища поширення акустичних коливань і способів їхнього перехоплення технічні канали витоку акустичної (мовний) інформації можна розділити на повітряні, вібраційні, електроакустичні, оптико-електронний і параметричні. Витік акустичної інформації за межі огороджувальних конструкцій можливий трьома шляхами (рис. 8.1):

- за рахунок «мембранного ефекту»;
- через тріщини, отвори, щілини та інші акустичні отвори, тобто прямим розповсюдженням акустичних коливань;
- за рахунок перетворення акустичних коливань в віброакустичні, а потім знов в акустичні.

У даному випадку частина енергії акустичних коливань, падаючи на поверхню огороджувальної конструкції,перетворюється на віброакустичні, тобто в коливання твердих частинок матеріалу без перенесення речовини.

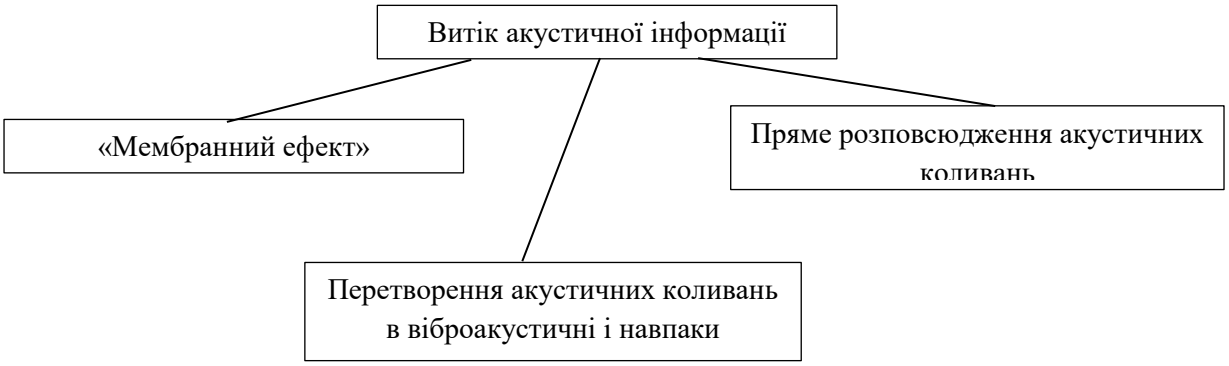

Рисунок 8.1 – Шляхи витоку акустичної інформації

Подолавши огороджувальну конструкцію, частина енергії віброакустичних коливань (частина відбивається) перетворюється на акустичну і випромінюється у вигляді акустичних коливань. Схематично канали витоку акустичної інформації відображені на рисунку 8.2.

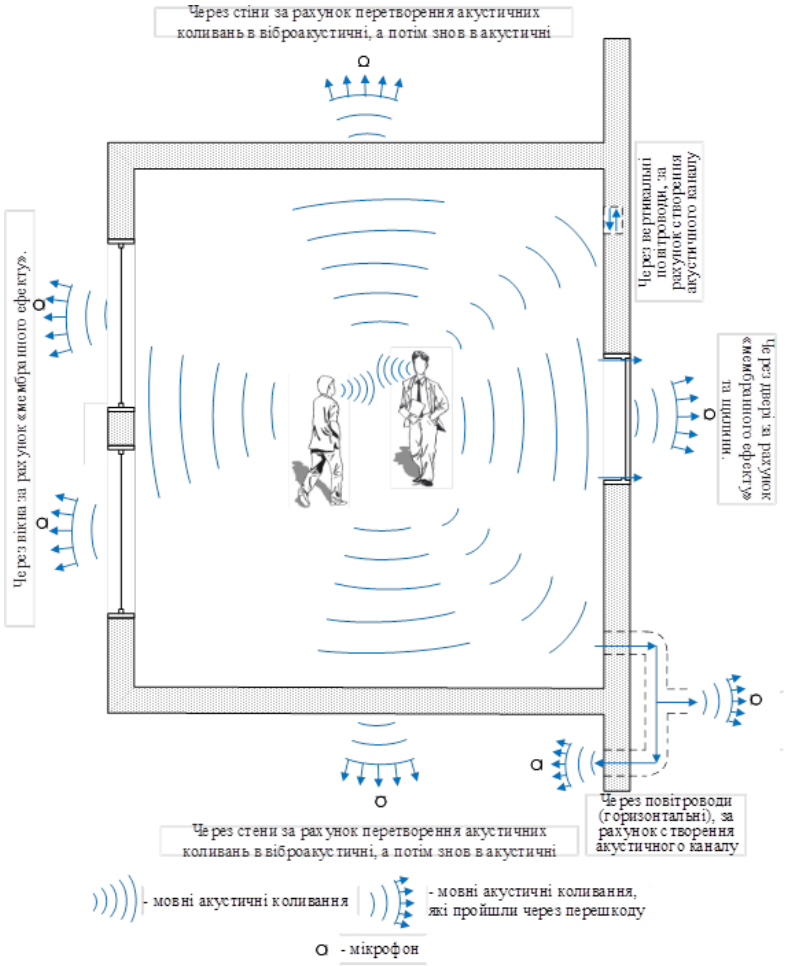

Рисунок 8.2 – Канали витоку акустичної інформації

Приймання акустичної інформації можливо без використання засобів технічної розвідки при випадковому прослуховуванні (тобто без умисних дій, спрямованих на отримання цієї інформації), а також з використанням засобів

технічної розвідки.

Для перехоплення акустичної інформації можуть використовуватися високочутливі мікрофони. Якщо немає можливості застосувати такі мікрофони використовуються спрямовані мікрофони, тобто таки, які мають вузьку діаграму спрямованості.

Перехоплена мовна інформація може записуватися на портативні записуючі пристрої (диктофони) або передаватися по радіоканалу, мережі електроживлення, оптичному каналу з'єднувальним лініям, стороннім провідникам, інженерним комунікаціям тощо.

8.3 Віброакустичні канали

Перехоплення інформації, перетвореної з повітряної в вібраційну (структурну), може бути здійснено безпосередньо з несучих конструкцій якими є огороджувальні будівельні конструкції приміщень (стіни, вікна, двері, перекриття тощо) а також інженерні комунікації (рис. 8.3).

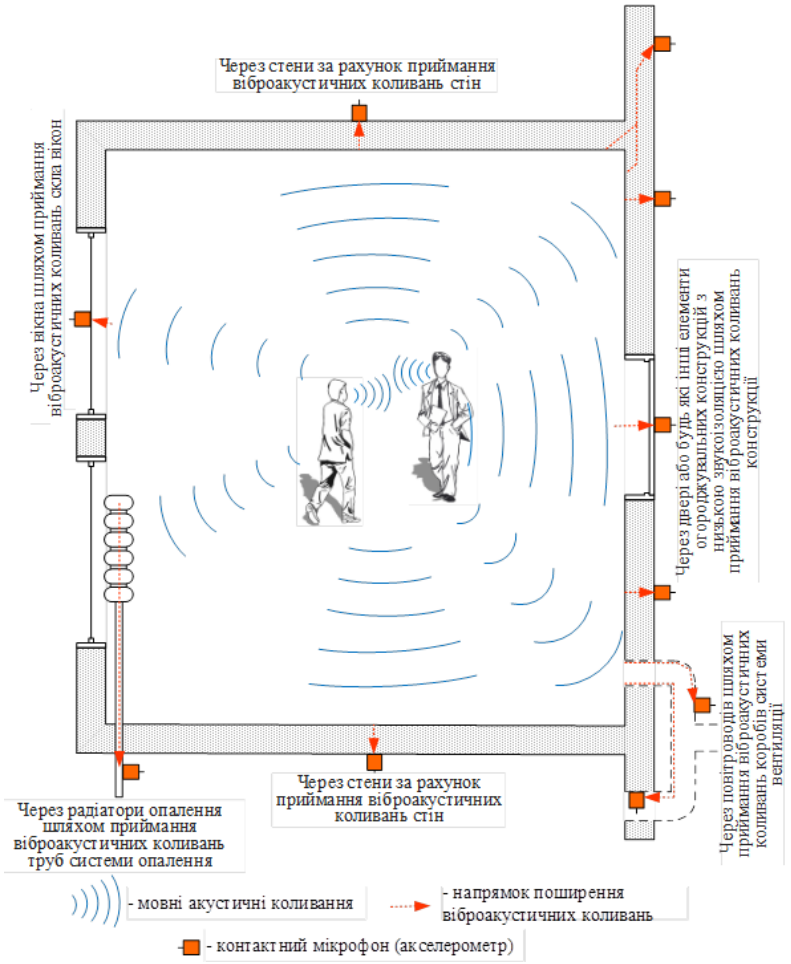

Рисунок 8.3 - Віброакустичні канали витоку інформації

Відповідно шлях інформації від джерела до пристрою перехоплення буде мати вигляд: джерело –> середовище (повітря) –> тверда середовище –> ТЗР. Для

перехоплення мовних сигналів у цьому випадку використовують контактні мікрофони (акселерометри). Вібродатчик, з'єднаний з електронним підсилювачем називають електронним стетоскопом (ЕС). ЕС дозволяє здійснювати прослуховування мови за допомогою телефонів та її запис.

По віброакустичному каналу також можливо перехоплення інформації з використанням засобів перехоплення (ЗП). Для передачі інформації часто використовується радіоканал, тому такі пристрої часто називають радіостетоскопами.

Можливе використання ЗП з передачею інформації по оптичному каналу в ближньому інфрачервоному діапазоні довжин хвиль, а також по ультразвуковому каналу (по інженерним комунікаціям).

8.4 Акустоелектричні канали

При організації захисту акустичної (мовної) інформації необхідно враховувати можливість її витоку з систем звукопідсилення, магнітного звукозапису, при передачі по каналах зв'язку, систем звукового супроводу кінофільмів і т.п. Витік акустичної інформації може статися через вплив акустичного сигналу на елементи тракту радіоелектронних систем - конденсатори, котушки індуктивності, елементи телефонного апарату, вторинних годинників і т.п. У цьому випадку перетворений в електричний інформаційний акустичний сигнал може поширюватися на великі відстані (рис.8г). Середовище - "повітря - електроакустичний перетворювач - повітря (або струмопровідні ланцюги)". ТЗР - приймач електричних сигналів або електромагнітних хвиль. Акустоелектричні канали витоку інформації виникають за рахунокперетворень акустичних каналів в електричні (рис. 8.4).

Деякі елементи допоміжних технічних засобів і систем (ДТЗС), у тому числі трансформатори, котушки індуктивності, електромагніти вторинних годинників, телефонних апаратів і тощо, мають властивість змінювати свої параметри (ємність, індуктивність, опір) під дією акустичного поля, створюваного джерелом мовного сигналу.

Зміна параметрів призводить або до появи на даних елементах електрорушійної сили (ЕРС), або до модуляції струмів, що протікають по цим елементам згідно із змінами електричного поля.

Технічний канал витоку інформації з використанням «високочастотного електромагнітного нав'язування» може бути здійснено шляхом несанкціонованого контактного введення струмів високої частоти від генератора в лінію, що має функціональні зв'язки з нелінійними або параметричними елементами ДТЗС, на яких відбувається модуляція високочастотного каналу інформаційним сигналом.

Інформаційний сигнал у даних елементах ДТЗС з'являється внаслідок акустоелектричного перетворення акустичних сигналів в електричні.

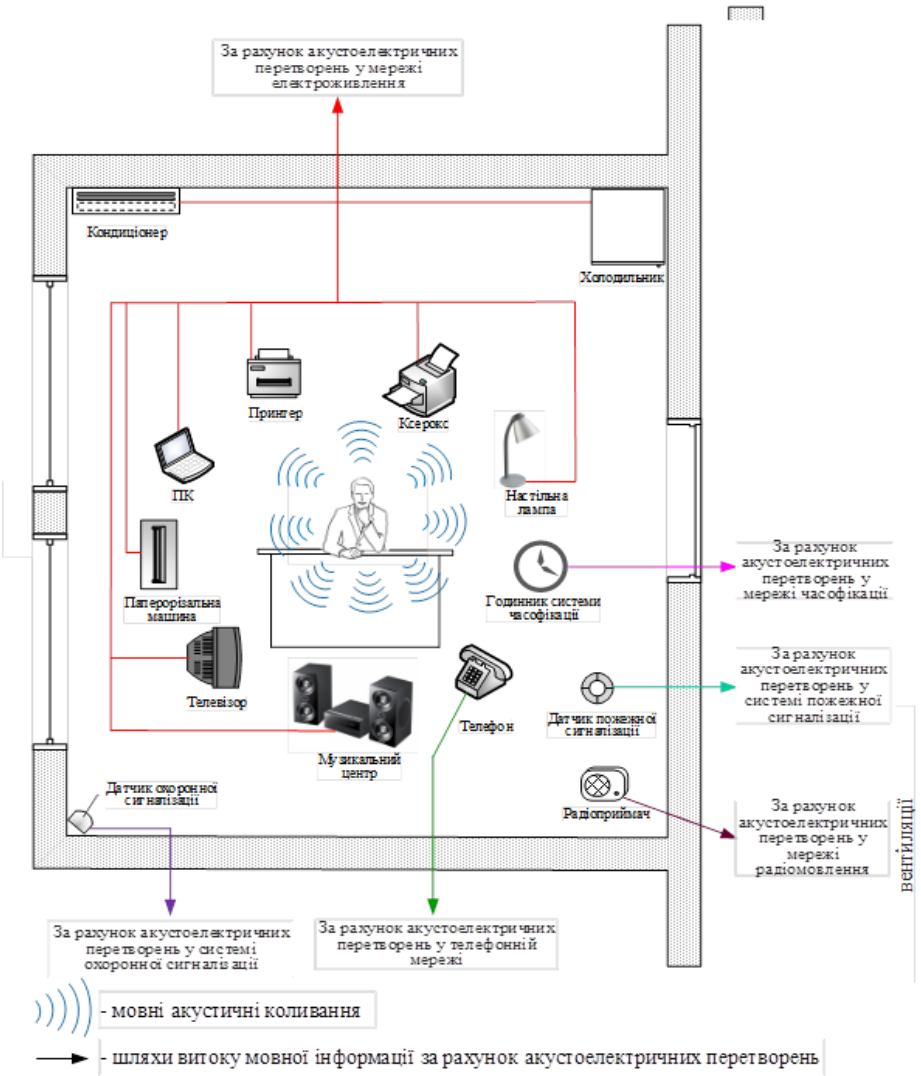

Рисунок 8.4 - Канали витоку акустичної інформації за рахунок акустоелектричних перетворювань

Промодульований сигнал відбивається від зазначених елементів і поширюється у зворотному напрямку або випромінюється.

8.5 Оптико - електронний (лазерний) канал

Оптико - електронний (лазерний) канал витоку акустичної інформації утворюється при опроміненні лазерним променем вібруючих під дією акустичного мовного сигналу відбиваючих поверхонь приміщень (шибок, дзеркал тощо). Відбите лазерне випромінювання модулюється по амплітуді або фазі і приймається приймачем оптичного (лазерного) випромінювання, при демодуляції якого виділяється мовна інформація (рис. 8.5).

В оптичному каналі отримання інформації можливо шляхом:

- візуального спостереження,
- фото-відеозйомки,
- використання видимого і інфрачервоного діапазонів для передачі інформації від приховано встановлених мікрофонів та інших датчиків.

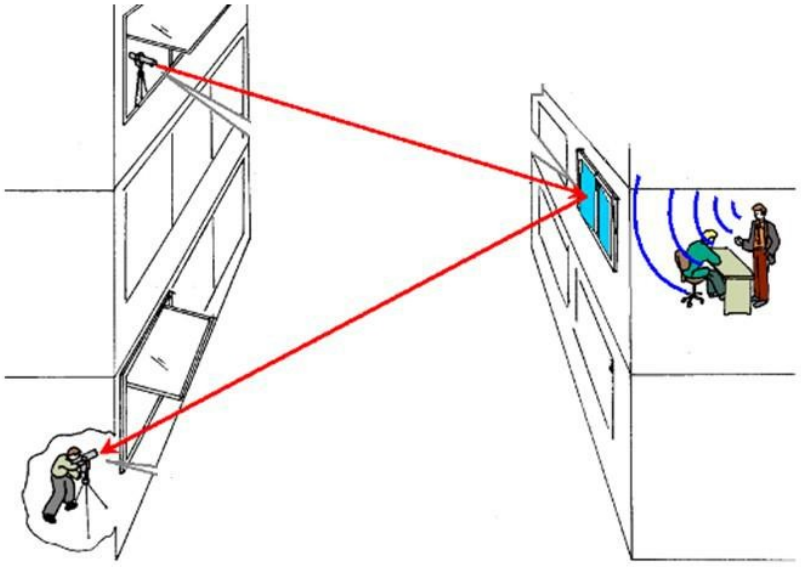

Рисунок 8.4 - Канали витоку акустичної інформації за допомогою оптико-електронних пристроїв перехоплення інформації

Як середовище поширення в оптичному каналі витоку інформації виступають:

- безповітряний простір;
- атмосфера;
- оптичні світловоди.

Безповітряний простір, що є середовищем поширення витоку інформації, виникає при спостереженні за наземними об'єктами з космічних апаратів. До властивостей середовища поширення, що впливають на довжину каналу витоку, відносяться:

- характеристики прозорості середовища поширення;
- спектральні характеристики світла. Для організації такого каналу є кращим використання дзеркального відбиття лазерного променю.

Однак, при невеликих відстанях до поверхонь, що відбивають (порядку декількох десятків метрів) може бути використано дифузне віддзеркалення лазерного випромінювання.

Складні лазерні системи - «лазерні мікрофони», які працюють, як правило в ближньому інфрачервоному діапазоні довжин хвиль.

8.6 Параметричні канали

У результаті впливу акустичного поля змінюється тиск на всі елементи високочастотних генераторів основних технічних засобів прийому, обробки, зберігання та передачі інформації (далі – ОТЗ) і ДТЗС. При цьому змінюється взаємне розташування елементів схем, проводів в котушках індуктивності, дроселів тощо, що може призвести до змін параметрів високочастотного сигналу, наприклад, до модуляції його інформаційним сигналом. Тому цей канал витоку інформації

називається параметричним.

Найбільш часто спостерігається паразитна модуляція інформаційним сигналом випромінювань гетеродинів радіоприймальних і телевізійних пристроїв, які перебувають у приміщеннях, де ведуться конфіденційні переговори. Параметричний канал витоку інформації утворюється шляхом «високочастотного опромінювання» ТЗПІ. Для перехоплення інформації по даному каналу необхідні спеціальні високочастотні генератори з антенами або встановлені закладні пристрої, що мають елементи, параметри яких (наприклад, добротність і резонансна частота об'ємного резонатора) змінюються під дією акустичного (мовного) сигналу і спеціальні радіоприймальні пристрої.

При опроміненні приміщення потужним високочастотним сигналом в такому ЗП при взаємодії електромагнітного поля зі спеціальними елементами закладки відбувається утворення вторинних радіохвиль, тобто перевипромінювання електромагнітного поля. А спеціальний пристрій закладки (наприклад, об'ємний резонатор) забезпечує амплітудну, фазову або частотну модуляцію переотраженного сигналу за законом зміни мовного сигналу. Для реалізації можливостей такого каналу необхідні спеціальний передавач з направленим випромінюванням.

9. ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ НА ОСНОВІ ЗАКЛАДНИХ ПРИСТРОЇВ

9.1. Сутність та класифікація засобів несанкціонованого перехоплення інформації (закладних пристроїв).

9.2. Загальні характеристики та особливості деяких типів закладних пристроїв.

9.3. Заходи захисту інформації від витоку каналами на основі закладних пристроїв.

9.1 Сутність та класифікація засобів несанкціонованого перехоплення інформації (закладних пристроїв)

Одним зі шляхів витоку, а точніше можливостей перехоплення противником інформації на об’єкт інформаційної діяльності (ОІД) є витік інформації через засоби несанкціонованого перехоплення.

Сутність їх полягає в тому, що вони знаходячись в межах КЗ ОІД приймають (перехоплюють) сигнал, щоциркулює, та передають його противнику.

Засоби несанкціонованого перехоплення приховано розміщують на об'єкті та камуфлюють під звичайні предмети та інші елементи так, щоб їх було складно виявити.

Умовно цей канал витоку можна зобразити у вигляді рисунку 9.1.

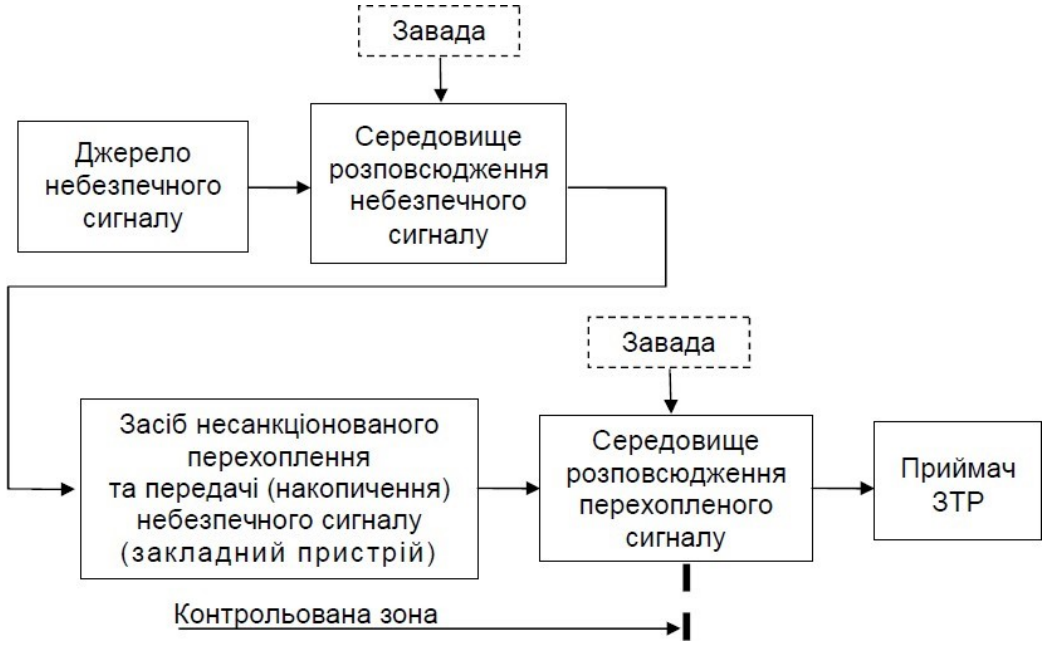

Рисунок 9.1 - Канали витоку інформації на основі закладних пристроїв

Розміщення засобів несанкціонованого перехоплення на ОІД або вмежах КЗ можливе шляхом (рис. 9.2):

— несанкціонованого проникнення на ОІД (в КЗ) сторонніх осіб;

— порушення правил режиму доступу штатних осіб на ОІД;

— закладки цих засобів у приміщенні до (під час) обладнання в них ОІД та комплексу ТЗІ.

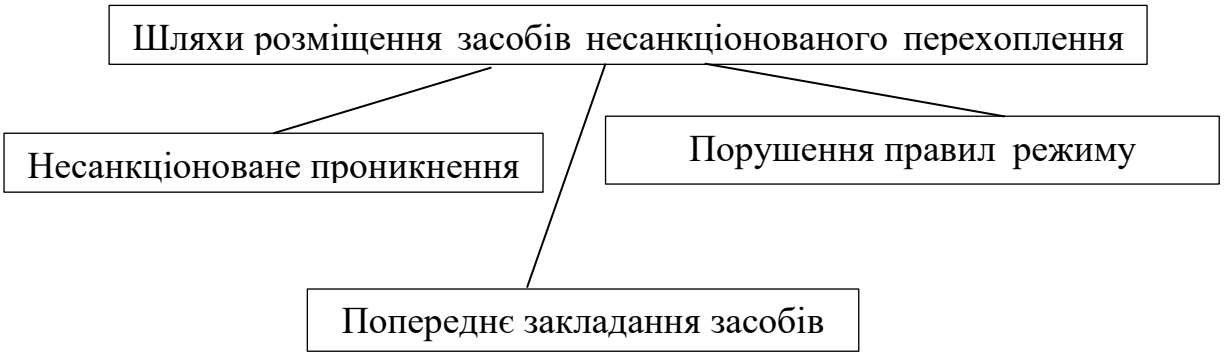

Рисунок 9.2 - Шляхи розміщення засобів несанкціонованого перехоплення

Тому засоби несанкціонованого перехоплення, отримали назву закладних пристроїв, саме так їх називають у сучасній літературі та підручниках (рис. 9.3, 9.4).

Закладні пристрої класифікують: **за видом та способом прийому інформації** та **за способом передачі перехопленої інформації до приймача** ТЗР противника.

За видом та способом прийому інформації закладні пристрої розділяють на:

— закладні пристрої, призначені для одержання мовної акустичної інформації, що циркулює в приміщенні (аудіо-закладні пристрої);

— закладні пристрої, призначені для одержання аудіо- та відео-інформації (телевізійні закладні пристрої);

— закладні пристрої з підключенням до телефонних ліній зв'язку, пристроям обробки та передачі інформації та ін.

Рисунок 9.3 - Класифікація закладних пристроїв

Рисунок 9.4 - Класифікація пристроїв несанкціонованого зняття інформації

За способом передачі перехопленої інформації противнику закладні пристрої розділяють на:

— закладні пристрої, що використовують для передачі перехопленої інформації радіоефір (радіо-закладні пристрої);

— закладні пристрої з передачею перехопленої інформації по мережам зв'язку, управління, живлення і т. п.;

— радіо-закладні пристрої з перевипромінюванням (пасивні);

— закладні пристрої з передачею перехопленої інформації по стандартному телефонному каналу - так названі закладні пристрої типу «довге вухо», або «зі штучно піднятою трубкою» та ін.

9.2. Загальні характеристики та особливості деяких типів закладних пристроїв

Загалом виділяють наступні характеристики закладних пристроїв.

1. **Оформлення (виконання) або спосіб монтажу:**

- прихований монтаж при попередньому розміщенні закладного пристрою;
- при незаконному проникненні у вигляді різноманітних технічних модулів чи складових приладів закамуфльованих під технічні елементи та пристрої, елементи одягу, побутові предмети та ін.

2. **Потужність випромінювання:**

- до 10 мВт - мала потужність;
- від 10 до 100 мВт - середня потужність;
- більше 100 мВт - велика потужність;
- з регульованою потужністю випромінювання.

3. Використовуваний вид модуляції: АМ, РМ, WFM (широкосмугова), ІЧРМ (вузькосмугова) та ін.

4. **Стандарти модуляції:**

- модуляція з інверсією спектру;
- модуляція з частотною мозаїкою;
- дельта-модуляція;
- модуляція в шумоподібні сигнали.

5. **Стабілізація частоти:**

- нестабілізовані;
- зі схемотехнічною стабілізацією частоти;
- з кварцовою стабілізацією.

6. **Гарантована дальність перехоплення або спосіб підключення:**

- до 10 м з посередництвом звукової хвилі через мікрофон, або з підключенням до мікрофонів (слухавок) пристроїв обробки та передачі інформації;
- до 1 м з посередництвом вібраційної хвилі (через цегельні й бетонні

стіни) та контактний мікрофон - стетоскоп;

- контактне підключення та установка закладних пристроїв перехоплення інформації в каналах обробки інформації, систем передачі даних та зв'язку.

Радіозакладні пристрої - це закладні пристрої, які для передачі перехопленої інформації до засобів ТЗР використовують радіоефір. Передача в них здійснюється шляхом перетворення (модуляції) перехоплених сигналів в електромагнітні хвилі, що розповсюджуються в просторі - ефірі.

Для виявлення випромінюючих в ефір радіозакладок необхідне визначення діапазону їхньої роботи, виду модуляції та закриття.

Суттєве ускладнення в пошуку закладних пристроїв також викликають види модуляції й закриття (скремблювання, рандомізація, шифрування, тощо), які постійно змінюються і удосконалюються.

Закладні пристрої типу «довге вухо» або закладка «зі штучно піднятою трубкою» - це закладні пристрої, які комплексуються з абонентськими пристроями телефонного зв’язку загального користування, що знаходяться на ОІД, та можуть дистанційно керуватися з використанням цієї ж телефонної мережі.

При покладеній трубці телефонного апарату до лінії підключена система виклику, яка приймає у випадку виклику абонента сигнал виклику. Коли абонент піднімає трубку, система виклику відключається, до лінії підключається переговорна система телефонного апарату і забезпечується зв'язок. Закладка з «штучно піднятою трубкою» забезпечує підключення переговорної систем телефонного апарату з мікрофоном трубки, або додаткового мікрофона до лінії без механічного підйому трубки. Подача сигналу для штучного підйому трубки може здійснюватися різними способами. Наприклад:

- *набирається номер абонента,* якому встановили в телефонний апарат закладку для прослуховування;
- *після декількох сигналів виклику кладеться трубка* так, щоб абонент не встиг її підняти, ніби хтось помилився, і система виклику у телефонному апараті з закладкою відключається;
- *через певний інтервал часу (10...40 с) здійснюється повторний виклик.* При цьому для того щоб сторонній виклик, що випадково потрапив у цей інтервал часу, не підключився до системи, на протязі 45...60 с закладка виробляє сигнал відбою;
- через зазначений інтервал часу (45...60 с) *закладний пристрій підключається до лінії,* і йде контроль акустики приміщення (слід зазначити, що при підключенні до телефонного апарата додаткових мікрофонів може бути організований контроль інших приміщень);
- при піднятті трубки абонента, що прослуховується, закладка відключається.

Відомі й інші способи несанкціонованого підключення телефонів із закладкою

до лінії, особливо для сучасних цифрових систем обслуговування.

Суттєвою особливістю закладних пристроїв типу «довге вухо» або

«зі штучно піднятою трубкою» є їхня велика дальність дії - практично по всій земній кулі.

Радіозакладні пристрої з перевипромінюванням - це закладнірпристрої, які реалізують перевипромінювання ВЧ поля з модуляцією йогонебезпечним сигналом, що циркулює на ОІД. Як правило, даний тип закладок використовується для перехоплення мовних акустичних сигналів.

Структура цією закладки складається з двох резонаторів: електромагнітного ВЧ резонатора та акустичного, налаштованого на частоту мовного сигналу. Вказані резонатори взаємодіють так, що акустичний,знаходячись під впливом поля мовного сигналу, вібрує та приводить до зміни добротність електромагнітного ВЧ резонатора. В результаті перевипромінення відбувається модуляція.

Суттєвою особливістю такого пристрою є те, що він не використовує джерела електроживлення і може працювати необмежено довго. Крім того сама закладка не випромінює, якщо немає поля опромінення, що ускладнює її пошук.

Мережеві закладні пристрої - це закладні пристрої, які для свого функціонування використовують мережу електроживлення. їх умовно розділяють на дві групи:

— закладні пристрої, що для передачі перехопленої інформації використовують мережу електроживлення як середовище;

— закладні пристрої, що живляться від мережі електроживлення і для передачі перехопленої інформації використовують не мережу електроживлення, а інше середовище, наприклад, радіоефір.

Ці закладки, як правило, камуфлюються під побутові прилади (електролампа, електрочайник, тощо), і можуть бути досить просто впровадженими на ОІД. Включення заставних пристроїв забезпечується, як правило, включенням камуфлюючого пристрою у мережу.

Однієї з суттєвих особливостей подібних закладних пристроїв є необмежений час їхньої роботи (поки є мережа живлення).

Однак для таких пристроїв існує ряд обмежень. Наприклад, не рекомендується використовувати камуфлюючий виріб з великим споживанням електроенергії, більше 0,5 кВт. Це може викликати в акустичному каналі заважаючий мережевий фон. Не рекомендується встановлювати радіомікрофон поблизу джерел акустичних завад: холодильника, вентилятора, трансформатора, телевізора й т.п.

Для забезпечення більшої прихованості закладних пристроїв може бути використане дистанційне управління, що дозволяє включати закладний пристрій тільки на необхідний час.

9.3. Заходи захисту інформації від витоку каналами на основі закладних пристроїв

Канали витоку інформації на основі закладних пристроїв є рукотворними технічними каналами витоку, призначеними для несанкціонованого перехоплення інформації. Тому при їх установці, вживають заходи для маскування різними способами. Маскування закладних пристроїв істотно ускладнює їхпошук і захист від витоку інформації. Для захисту інформації від витоку каналами на основі закладних пристроїв проводяться такі заходи:

— недопущення установки закладних пристроїв на ОІД;

— виявлення та протидія роботі закладних пристроїв на ОІД.

Зазначені заходи розрізняють на організаційні та технічні.

Організаційні заходи (глобальні) включають:

— організацію режиму роботи виділених приміщень та ОІД;

— організацію контролю за доступом відвідувачів і співробітників, що мають обмеження за доступом;

— організацію контролю роботи співробітників;

— організацію перевірки приміщень об'єкта і техніки, що перебуває на ньому, на наявність закладних пристроїв, у тому числі інової, що поступає;

— аналіз методів і способів установки закладних пристроїв, їхнього камуфляжу, конструкцій та технологій.

Технічні заходи (глобальні) включають:

— створення системи технічних засобів охорони;

— створення системи охоронної сигналізації;

— створення телевізійної системи спостереження;

— створення системи контролю керування доступом;

— використання технічних засобів, що сигналізують про підключення в виділених приміщеннях закладних пристроїв долінії зв'язку, мережі живлення і т.п.;

— використання технічних засобів контролю на наявність закладних пристроїв у техніці, що поступає, та приміщеннях;

— використання технічних засобів контролю радіовипромінювань та випромінювань у лініях зв'язку, живлення та керування;

— використання технічних засобів контролю інфрачервоних випромінювань;

— використання технічних засобів нелінійної радіолокації та підповерхневої локації;

— використання рентгенівських установок, тепловізійних систем, металодетекторів, тощо.

При пошуку закладних пристроїв застосовують різноманітні методи, які можна розділити на пошук як фізичних та пошук як електронних засобів (рис. 9.5).

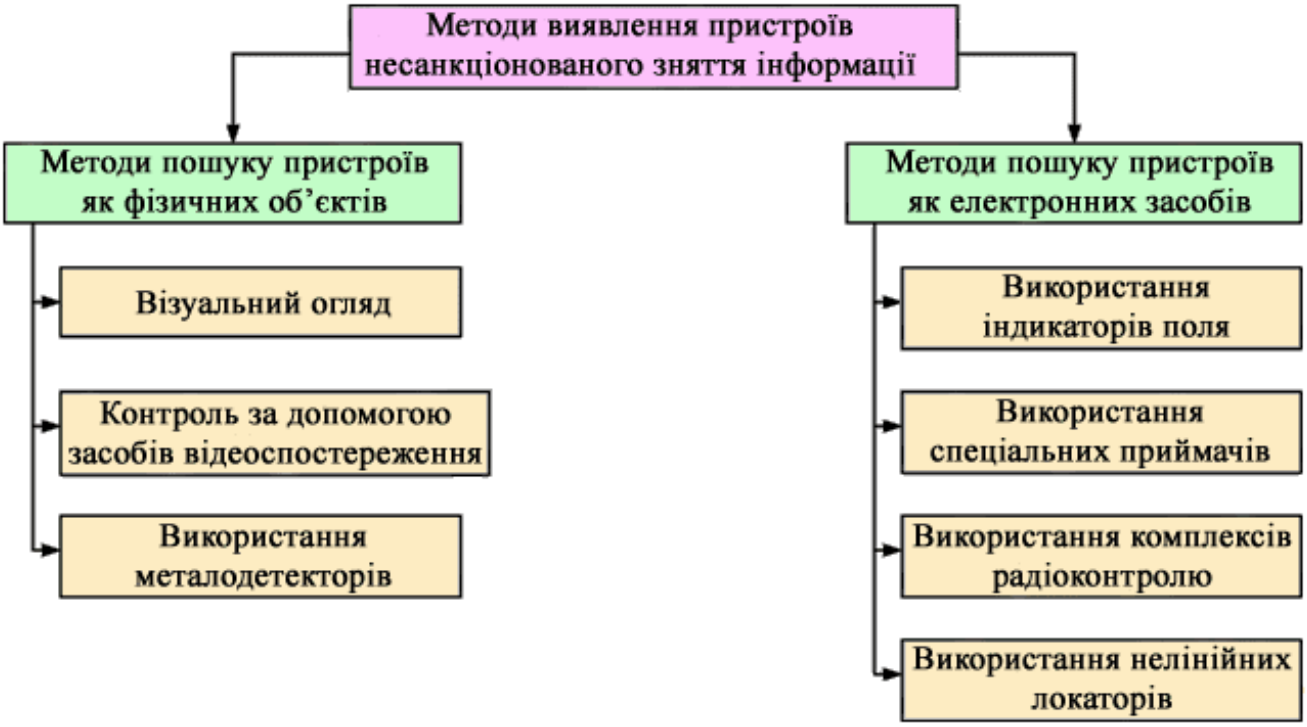

Рисунок 9.5 – Методи виявлення пристроїв несанкціонованого зняття інформації

Окрім глобальних організаційних заходів, які є в більшій мірі нормативами для роботи підприємства чи організації, розглядають також локальні організаційні заходи. Вони включають в себе:

- аналітичну роботу з виявлення можливих місць установки закладних пристроїв (з урахуванням особливостей їхньої роботи);
- організацію роботи служби безпеки по контролю випромінювань в ефірі, мережах зв'язку, управління;
- аналіз частотного діапазону й способів роботи закладних пристроїв.

Локальні технічні заходи включають різноманітні заходи, пов'язані з виявленням закладних пристроїв та безпосередній захист як от:

- контроль сигналів у лініях зв'язку, керування, живлення, охоронних систем;
- контроль радіовипромінювань у районі ОІД;
- контроль інфрачервоних випромінювань у районі розташування ОІД;
- використання апаратури нелінійної радіолокації та підповерхневої локації;
- використання рентгенівських установок, тепловізійних систем, металодетекторів;
- використання технічних засобів, що сигналізують про підключення закладних пристроїв;
- використання засобів візуального контролю;
- (заходи, пов'язані з протидією роботі закладних пристроїв)

- використання електромагнітних засобів зашумлення;
- використання акусто-вібраційного зашумлення;
- демонтаж, руйнування та відключення закладних пристроїв.

10. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ВІД СПОСТЕРЕЖЕННЯ ТА ПІДСЛУХОВУВАННЯ

10.1. Засоби протидії спостереженню в оптичному діапазоні та радіолокаційному спостереженню.

10.2. Енергетичне приховування акустичного сигналу.

10.3. Засоби звукоізоляції та звукопоглинання.

10.4. Класифікація засобів виявлення та локалізації закладних пристроїв.

10.1. Засоби протидії спостереженню в оптичному діапазоні та радіолокаційному спостереженню

Об'єкт спостереження в оптичному каналі витоку інформації є і джерелом інформації, і джерелом сигналу, оскільки світлові промені, що несуть інформацію про видові характеристики об'єкта, відбиваються променями об'єкта зовнішнього джерела або його власного випромінювання.

Відбите від об’єкта світло містить інформацію про його зовнішній вигляд (видові характеристики), а світло, що випромінюється об’єктом, – про параметри випромінювання (характеристики сигналу). Інформація записується в момент відбиття падаючого світла шляхом зміни його яскравості та спектрального складу. Випромінюване світло містить інформацію про рівень і спектральний склад видимих джерел світла, а в інфрачервоному діапазоні про характеристики випромінювання можна також судити по температурі елементів випромінювання.

Довжина (протяжність) каналу джерела залежить від потужності світла від об'єкта, властивостей середовища поширення та чутливості фотоприймача.

Середовище поширення в оптичному каналі витоку інформації буває трьох типів:

- безповітряний (космічний) простір;
- атмосфера;
- оптичні канали.

Оптичний канал витоку інформації, середовище поширення якого містить ділянки безповітряного простору, виникає при спостереженні наземних об'єктів з космічних апаратів. Межа між космосом і атмосферою досить умовна. На висотах 200-300 км ще залишаються залишки газів, які проявляються в гальмівному впливі на космічні кораблі.

Метеорологічна видимість навіть у вікнах прозорості залежить від наявності в атмосфері зважених частинок пилу і вологи, що утворюють туман і туман, крапель і кристалів води у вигляді дощу і снігу, а також аерозолів і диму, що містять тверді

речовини. частинок. Все це викликає помутніння атмосфери і погіршує видимість.

Властивості середовища поширення, які впливають на довжину каналу витоку, включають(рис. 10.1):

- характеристику прозорості середовища розповсюдження;
- спектральні характеристики світла.

Рисунок 10.1 - Шкала довжин хвиль

Ослаблення світла при проходженні через атмосферу характеризується коефіцієнтом пропускання.

У промисловості і побуті набули масового застосування прилади та обладнання, робота яких пов'язана з використанням або утворенням в процесі роботи електромагнітних випромінювань оптичного діапазону, до яких належать електромагнітні коливання з довжиною хвиль від 0,2 мкм до 1000 мкм.

Залежно від довжини хвилі ці випромінювання поділяються на:

- випромінювання видимого діапазону;
- інфрачервоні;
- ультрафіолетові лазерні (монохроматичні та видимого і суміжних з ним діапазонів).

Донедавна атмосфера і безповітряний простір були єдиним середовищем для поширення світлових хвиль. З розвитком волоконно-оптичних технологій в оптичному діапазоні з’являються направляючі, які є більш досконалими для передачі великих обсягів інформації. Вони стійкі до зовнішніх перешкод, мають низьке загасання, довговічні, забезпечують набагато більшу безпеку інформації, що передається по волокну.

Будь-яке волокно характеризується двома важливими параметрами: ослабленням і дисперсністю. Загасання вимірюється в децибелах на кілометр (дБ / км) і визначається втратами на поглинання і розсіювання випромінювання в оптичному волокні.

Дисперсія, тобто залежність швидкості поширення сигналу від довжини хвилі, погіршує якість сигналу, а отже, і інформацію на виході довгого волокна. Дисперсія обмежує діапазон передачі та верхню частоту переданого сигналу.

Волокна об'єднані в волоконно-оптичні кабелі, покриті захисною оболонкою. Хоча ймовірність витоку інформації з волоконно-оптичного кабелю значно нижча, ніж з електричного, але за певних умов такий витік можливий. Для захоплення інформації в точці доступу до кабелю зруйнуйте його захисну оболонку, притисніть фотоприймач приймача до очищеної ділянки і зігніть кабель під кутом, під яким частина світлової енергії спрямовується на фотоприймач приймача.

Для спостереження **радіолокації** (Р) використовують: ехо-камерасигнали, віддзеркалення , що утворюються в результаті, радіохвиль від об'єкту, опроміненого станцією радіолокацій (РЛС) (т.з. Р. із зондуючим випромінюванням); сигнали РЛС, опромінюючe ретранслюючим пристроєм, що знаходиться на об'єкті, місце розташування якого визначається (Р. з активною відповіддю); власне радіовипромінювання об'єкту — випромінювання радіопристроїв, що знаходяться на об'єкті, або теплове випромінювання самого об'єкту, що визначається його температурою (пасивна радіолокація).

Серед багаточисельних принципів і методів радіолокації слід виділити найбільш важливі, пов'язані з дальністю дії РЛС, виміром дальності, пеленгацією, захистом від пасивних перешкод, дозволом. У основу першого способу покладено випромінювання імпульсу і вимір часу запізнювання відбитого об'єктом імпульсу відносно того, що випромінює. Вимір полегшується, якщо відбитий сигнал не накладається на той, що зондує, тобто об'єкт знаходиться на достатньому видаленні від РЛС. У простому випадку для реалізації цього способу застосовуються імпульсний передавач, приймач, задаючий генератор-синхронізатор для запуску передавача і задання шкали часу, індикатор осцилографічного типу, за шкалою якого можна визначати дальність. Модифікаціями цієї схеми є багатошкальні схеми побудовані за принципом ноніуса, і стежучі схеми - автодалекоміри.

В основу другого способу покладено спостереження інтерференції двох безперервних хвиль, пов'язаних із зондуючим випромінюванням і віддзеркаленням від об'єкту . При реалізації цього способу із зондуючими коливаннями, частота яких модульована по лінійному закону, в змішувач приймального пристрою поступають коливання передавача і сигналу, в результаті чого має місце биття між ними з частотою, пропорційній вимірюваній дальності. Після детектування, посилення і обмеження сигнали поступають на частотомір — лічильник частоти биття, шкала якого може бути проградуйована безпосередньо в одиницях дальності.

10.2. Енергетичне приховування акустичного сигналу

Енергетичне приховування акустичних сигналів відповідно до розглянутих способів захисту інформації забезпечується використанням методів і засобів, що зменшують енергію носія або підвищують енергію перешкод.

Найпростіший спосіб зробити це – зменшити гучність під час розмови на конфіденційні теми. Однак це можливо, якщо кількість співрозмовників невелика. В інших випадках використовується звукоізоляція, звукопоглинання та глушіння звуку. Третій спосіб передбачає використання активних засобів - генераторів акустичних перешкод.

Звукоізоляція спрямована на локалізацію джерел акустичних сигналів у закритому просторі в межах контрольованої зони. Основна вимога до нього полягає в тому, щоб за межами цієї зони відношення сигнал/шум не перевищувало максимально допустимих значень, що виключає отримання інформації зловмисниками. Часто ототожнюють поняття звукопоглинання та звукоізоляції, хоча між ними є принципова відмінність, яку необхідно враховувати при вирішенні практичних завдань у боротьбі з шумом. Найчастіше використовують метод звукопоглинання у виробничих приміщеннях.

Звукопоглинання — це зменшення енергії звукових хвиль, відбитих від зустрічних перешкод, внаслідок перетворення звукової енергії в теплову. Звукопоглинання застосовують, коли неможливо зменшити шум біля джерела.

Другий метод (глушіння звуку) передбачає застосування активних засобів - генераторів акустичних перешкод.

10.3. Засоби звукоізоляції та звукопоглинання

Звукоізоляція спрямована на локалізацію джерел акустичних сигналів в усередині контрольованої зони. Основна вимога - за межами зони співвідношення сигнал-перешкода не повинні перевищувати максимально-допустимі значення, що виключають добування інформації зловмисниками (рис. 10.2).

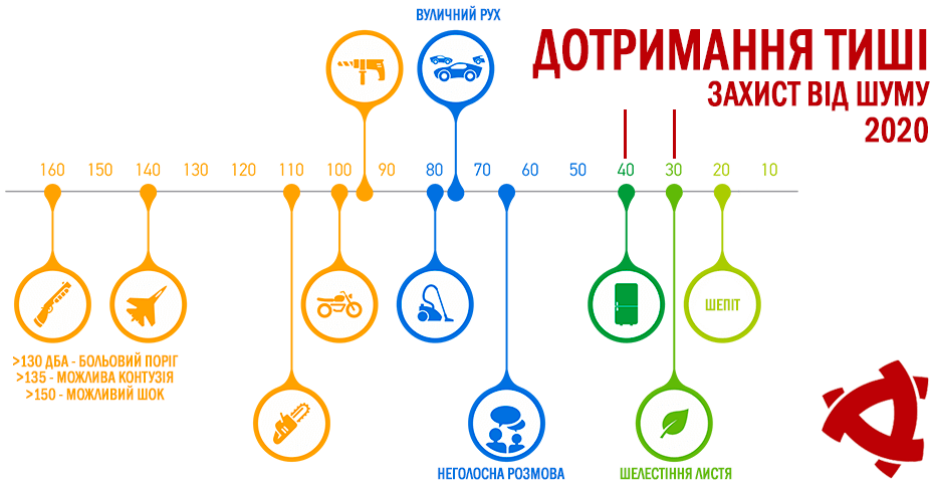

Рисунок 10.2 - Шкала гучності звуків

Звукоізоляція забезпечується за допомогою архітектурних і інженерних конструкцій: огорож, екранів, кабін, кожухів. При падінні акустичної хвилі на кордон поверхонь з різними питомими плотностями велика частина падаючої хвилі відбивається.

Менша частина хвилі проникає в матеріал звукоізолюючої конструкції і поширюється в ньому, втрачаючи свою енергію в залежності від довжини шляху і його акустичних властивостей матеріалу. Під дією акустичної хвилі звукоізолююча поверхня здійснює складні коливання, також поглинають енергію падаючої хвилі. Характер цих поглинань визначається співвідношенням частот падаючої акустичної хвилі і спектральних характеристик (розподілу частот) поверхні кошти звукоізоляції. В області резонансних частот (до 25-45 Гц) коштів звукоізоляції ослаблення залежить в основному від внутрішнього тертя в звукоізолюючому матеріалі, на більш високих частотах - від його поверхневої густини, вимірюваної в кг на 1 м 2 поверхні. З урахуванням діючих норм на звукоізоляцію в приміщенні поверхнева маса основних огороджувальних конструкцій повинна становити не менше 250-300 кг. Звукоізолюючі огорожі - це стіни, перекриття, перегородки, вікна, двері, що мають по периметру контакти з іншими огородженнями.

Величина звукоізоляції однорівневої огорожі характеризується складної нелінійної залежністю як від частоти fзв коливання акустичної хвилі, так і від великої групи характеристик огорожі. У загальному випадку цю залежність можна представити у вигляді такої функції: R = F (fзв, M, h / fог, R, v), де m - поверхнева маса огорожі; h - коефіцієнт втрат енергії в матеріалі; fог - Власна частота коливань огорожі; r - питома щільність матеріалу огорожі; v - швидкість звуку в матеріалі огородження

Одним з найбільш слабких звукоізолюючих елементів огороджувальних конструкцій виділених приміщень є двері і вікна. Двері мають істотно менші в порівнянні з основними конструкціями поверхневі щільності, а також зазори і щілини.

10.4. Класифікація засобів виявлення та локалізації закладних пристроїв

Виявити закладні пристрої можна завдяки спеціальним обстеженням і спеціальним перевіркам об'єктів ТЗПІ та виділених приміщень (рис. 10.3).

Методи виявлення закладних пристроїв можна розділити на:

1. Пасивні методи:

- установлення засобів і систем виявлення лазерного випромінювання (підсвітлення скла на вікнах);

- установлення стаціонарних детекторів диктофонів;

- розшук закладних пристроїв за допомогою індикаторів поля, інтерсепторів, частотомірів, сканувальних приймачів та комплексів контролю;

- організація радіоконтролю побічних електромагнітних випромінювань ТЗПІ.

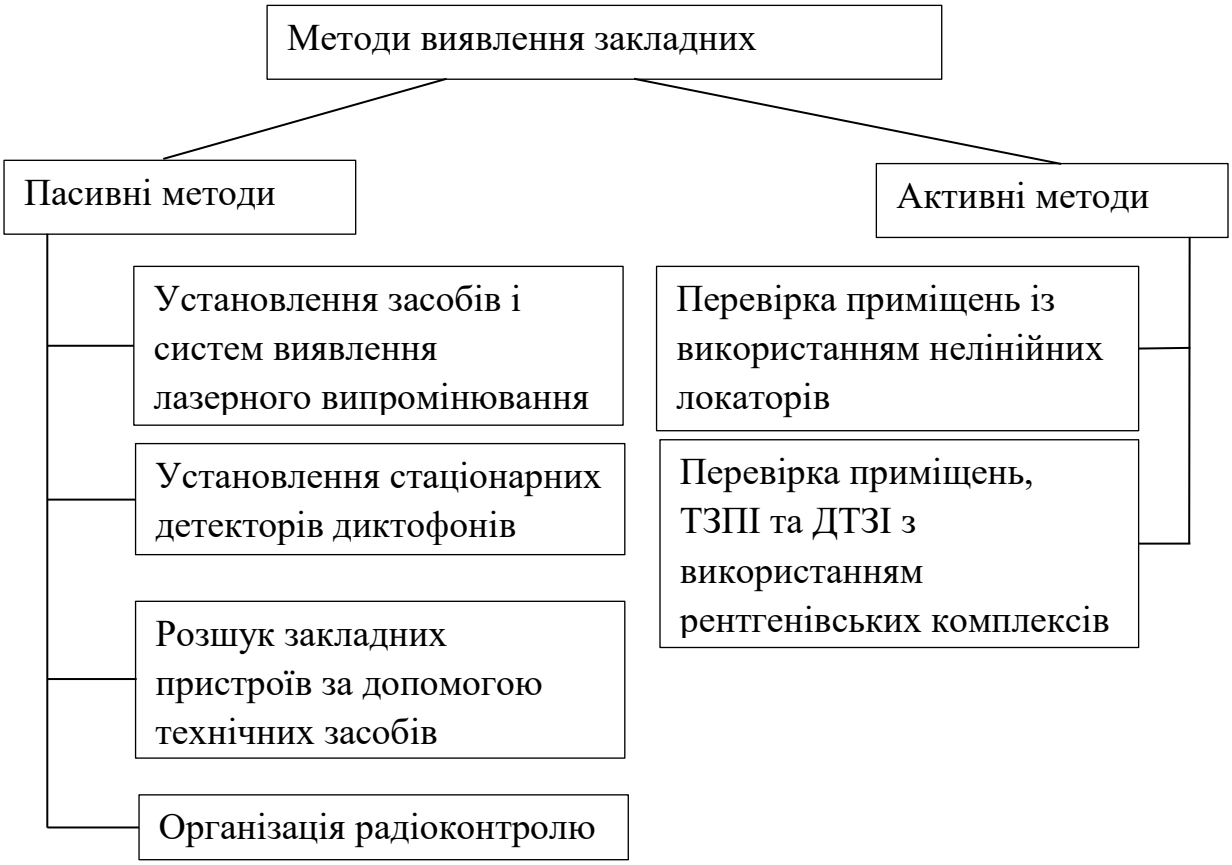

Рисунок 10.3 - Методи виявлення закладних пристроїв

2. Активні методи:

- спеціальна перевірка виділених приміщень із використанням нелінійних локаторів;

- спеціальна перевірка виділених приміщень, ТЗПІ та ДТЗІ з використанням рентгенівських комплексів.

Засоби радіоуправління приміщення призначені для виявлення закладних пристроїв, які випромінюють радіохвилі під час їх пошуку. Для виявлення невипромінюючих закладок при пошуку - дистанційно керованих і передачі сигналів по дротах використовуються засоби, які реагують не стільки на радіовипромінювання, скільки на інші демаскують ознаки закладок.

Методи та засоби виявлення не випромінюючих закладних пристроїв поділяються на дві групи:

1. **Перша група** - методи, засновані на пошуку ЗУ як фізичних об'єктів з цілком певними властивостями і малогабаритними характеристиками. До неї відносяться: - візуальний огляд місць можливого розміщення ЗУ, в тому числі із застосуванням збільшувальних стекол, дзеркал, засобів спеціального підсвічування; - контроль важкодоступних місць за допомогою засобів відео спостереження; - застосування метало детекторів.

2. **Друга група** - методи, які використовують властивості ЗУ як електронних систем. Вона включає: - використання індикаторів поля, що реагують

на наявність випромінювання радіо заставних пристроїв і дозволяють локалізувати їх розташування; - застосування спеціальних радіоприймальних пристроїв, призначених для пошуку сигналів за заданими характеристиками і аналізу електромагнітної обстановки; - застосування комплексів радіоконтролю і виявлення ЗУ; - обстеження приміщень за допомогою нелінійних радіолокаторів, що дозволяють виявляти будь-які типи ЗУ. Виявлення ЗУ як фізичних об'єктів є найбільш загальним випадком, що потрапляють під поняття огляду або огляду.

11. ЗАСОБИ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ПОБІЧНІ ЕЛЕКТРОМАГНІТНІ ВИПРОМІНЮВАННЯ

11.1. Придушення небезпечних сигналів акустоелектричних перетворювачів.

11.2. Екранування електромагнітних полів.

11.3. Запобігання витоку інформації по ланцюгам електроживлення

11.1. Придушення небезпечних сигналів акустоелектричних перетворювачів

Добре відомі способи отримання інформації про акустику приміщення за рахунок приєднання до ліній телефонних апаратів (особливо у випадках, коли в приміщенні розташовані апарати з електромеханічними викличними дзвінками), лініями диспетчерської або охоронної сигналізації і т.п.

Акустоелектричний перетворювач - це пристрій, що перетворює акустичну енергію (тобто енергію пружних хвиль в повітряному середовищі) в електромагнітну енергію в схемах тих пристроїв, в яких знаходяться акустоелектричні перетворювачі (або навпаки, енергію електромагнітних хвиль в акустичну) (рис. 11.1).

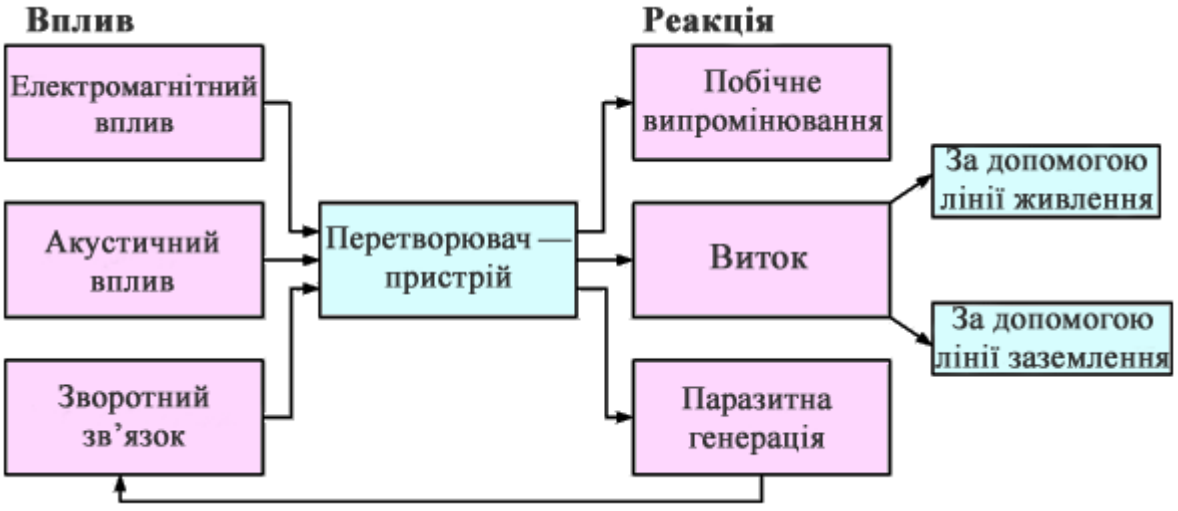

Рисунок 11.1 – Схема роботи акустоелектричного перетворювача

З оточуючих нас пристроїв найбільш відомі такі електроакустичні

перетворювачі:

- телефонні апарати (міського і внутрішнього зв'язку);
- системи провідної радіотрансляційної мережі;
- приймальні та телевізійні системи;
- системи звукозапису;
- внутрішній службовий зв'язок, переговорні пристрої типу "директор-секретар ";
- системи охоронної сигналізації;
- системи звукової сигналізації;
- системи електрогодинофікації і т.п.

Слід враховувати, що в більшості електроакустичних перетворювачів має місце подвійне перетворення енергії - електромеханічне, в результаті якого електрична енергія, що підводиться до перетворювача переходить в енергію коливань механічної системи (наприклад, дифузор динаміка), коливання якої і створює в середовищі звукове поле.

Для придушення акустоперетворюючого каналу витоку можуть бути використані організаційно-технічні і технічні способи захисту.

Організаційно-технічні заходи націлені на оперативне вирішення питань захисту конфіденційної акустичної інформації найбільш простими засобами і організаційними заходами обмежувального характеру, що регламентують порядок користування технічними засобами, що перебувають у виділених приміщеннях.

На етапі організаційно-технічних заходів щодо захисту від акустоперетворюючих каналів витоку інформації можуть бути вжиті заходи обмежувального характеру, що регламентують порядок користування технічними засобами, наприклад, відключення акустоперетворюючих елементів від провідних систем або відключення таких систем, що мають у своєму складі такі елементи.

Наприклад, відключення дзвінкових ланцюгів телефонних апаратів (всього телефонного апарату), вимкнення радіоприймальних і телевізійних пристроїв, систем провідної радіотрансляційної мережі і т.п. на період проведення конфіденційних заходів. Визначення контрольованої зони на цьому етапі дозволяє виділити найбільш небезпечні з точки зору витоку інформації пристрою і звернути на них особливу увагу і першочерговий захист технічними засобами захисту.

Організаційно-технічні заходи визначають можливу контрольовану зону на об'єкті, - зону, де гарантовано виключене перебування осіб, не допущених до охоронюваної інформації (не мають постійного або разового пропуску на об'єкт).

Стосовно до акустоелектричного каналу витоку інформації необхідна зона може бути значною, так як необхідно враховувати можливість витоку перетвореної інформації як по провідних каналах, так і по радіоканалу. Встановлення такої контрольованої великої зони можливо тільки для підприємств з досить великою

територією і потужними службами безпеки. Проведення подібних заходів спрямоване також на виключення з виділеного приміщення всіх технічних засобів, наявність яких не викликано виробничою необхідністю.

Технічні заходи з інженерно-технічного захисту інформації передбачають блокування каналів можливого витоку інформації інженерними спорудами, що зменшують величину небезпечного акустичного сигналу, що впливає на елемент акустичного перетворювача, або зменшують величину перетвореного в електромагнітний інформаційний сигнал.

Можливо також підвищення рівня шумового сигналу, що забезпечує умови придушення інформативного або акустичного, або перетвореного сигналу.

11.2. Екранування електромагнітних полів

Екранування є одним з найефективніших методів захисту від електромагнітних випромінювань. Під екрануванням розуміється розміщення елементів ІС, що створюють електричні, магнітні та електромагнітні поля, в просторово замкнутих конструкціях. Способи екранування залежать від особливостей полів, створюваних елементами КС при протіканні в них електричного струму.

Характеристики полів залежать від параметрів електричних сигналів в ІС. Так при малих токах і високих напружених в створюваному поле переважає електрична складова. Таке поле називається електричним (електростатичним). Якщо в провіднику протікає струм великої величини при малих значеннях напруги, то в поле переважає магнітна складова, а поле називається магнітним. Поля, у яких електрична і магнітна складові порівнянні, називаються електромагнітними.

При екранування магнітних полів розрізняють низькочастотні магнітні поля (до 10 кГц) і високочастотні магнітні поля. Низькочастотні магнітні поля шунтуються екраном за рахунок спрямованості силових ліній уздовж стінок екрану. До системи просторового зашумлення, застосовуваної для створення маскувальних електромагнітних перешкод, висуваються такі вимоги: - Система повинна створювати електромагнітні перешкоди в діапазоні частот можливих побічних електромагнітних випромінювань технічних засобів обробки і передачі інформації (ТМЗК);

- Створювані перешкоди не повинні мати регулярної структури; - Рівень створюваних перешкод (як по електричній, так і по магнітної складової поля) повинен забезпечити ставлення с / ш на кордоні контрольованої зони менше допустимого значення у всьому діапазоні частот можливих побічних електромагнітних випромінювань ТМЗК;

- Система повинна створювати перешкоди як з горизонтальною, так і з вертикальною поляризацією (тому вибору антен для генераторів перешкод приділяється особлива увага);

- На кордоні контрольованої зони рівень перешкод, створюваних системою просторового зашумлення, не повинен перевищувати встановлених норм по ЕМС.

11.3. Запобігання витоку інформації по ланцюгам електроживлення

Під час роботи технічних засобів обробки інформації в наслідок ємнісних та інших зв’язків на корпусах цих засобів може накопичуватися небезпечний для життя потенціал. Цей потенціал може змінюватися за законом небезпечного сигналу, і небезпечний сигнал просочується в ланцюги заземлення.

Основні способи перехоплення небезпечних сигналів в ланцюгах заземлення:

- Перехоплення небезпечного сигналу з низькоомних ділянок ланцюга заземлення. Наприклад, слабко зварювальний шов, окислення контактів, мала площа перетину шини заземлення.

- Зняття різниці потенціалів ґрунту по віддаленню від заземлювача – джерела небезпечного сигналу, що можливе у разі великого опору заземлення.

- Зняття потенціалу зі сторонніх провідників, о близько розташовані з заземлювачем та мають з ним ємнісний зв’язок.

Запобігання витоку інформації каналами побічних електромагнітних наведень на лінії електроживлення досягається шляхом:

- Електроживлення від автономних електричних джерел: електростанцій, акумуляторів, тобто не мають сторонніх споживачів.

- Використання в лінії електроживлення технічних засобів захисту, що затримують сигнали низького рівня, мережевих фільтрів, систем двигунгенератор.

- Використання лінійного зашумлення ліній електроживлення.

12. МЕТОДИ І ЗАСОБИ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В КАНАЛАХ ЗВ’ЯЗКУ

12.1. Структурне приховування мовної інформації в каналах зв’язку.

12.2. Засоби контролю телефонних ліній.

12.3. Перехват повідомлень в GSM каналах.

12.1. Структурне приховування мовної інформації в каналах зв’язку

Мовна (акустична) інформація, що передається по каналу зв'язку, міститься в інформаційних параметрах електричних і радіосигналів. Сигнали передаються по лініях зв'язку в аналоговій або цифровій формі.

Шифрування та **закриття** використовуються для структурного приховування мовної інформації в каналах зв'язку (рис. 12.1).

При **шифруванні** аналоговий мовний сигнал з мікрофонного входу буде перетворений в цифровий за допомогою аналого-цифрового перетворювача. При аналого-цифровому перетворенні амплітуда сигналу вимірюється через регулярні інтервали, які називають **кроком дискретизації**.

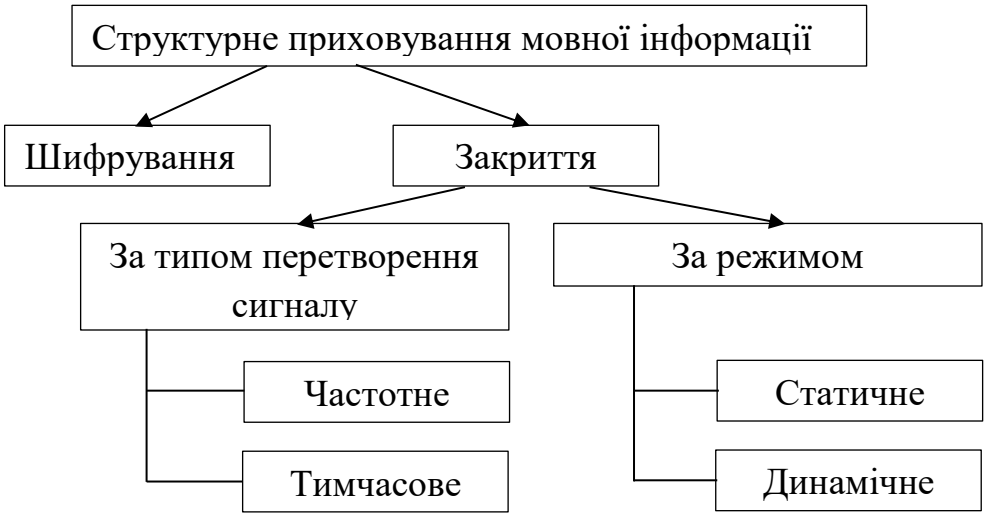

Рисунок 12.1 – Види структурного приховування мовної інформації

Щоб цифровий мовний сигнал мав якість не гіршу переданого по телефонному каналу в аналогової формі, крок дискретизації відповідно до теореми Котельникова повинен не перевищувати 160 мкс, а кількість рівнів квантування амплітуди цього сигналу — щонайменше 128.

З метою зниження необхідної швидкості розроблено різні методи стиснення мовного повідомлення. Методи стиснення використовують надмірність мовного сигналу або допускають зниження якості промови з допомогою показників, несуттєвих для семантики повідомлення.

Приховування голосового сигналу у вузько смуговому телефонному каналі здійснюється шляхом технічного або аналогового закриття.

За назвою технічних засобів, що забезпечують технічне закриття, ці методи ще називають **скремблюванням** (scrambling). Технічне закриття відрізняється від криптографічного тим, що шифрування приховує голосове повідомлення в символічній формі, а технічне закриття приховує голосовий сигнал без перетворення його в цифрову форму.

При технічному закритті ознаки вихідного мовного сигналу змінюються так, що він стає схожим на шум, але займає ту саму смугу частот. Це дозволяє передавати зашифровані сигнали через звичайний телефонний канал.

За типом перетворення сигналу розрізняють **частотний** і **тимчасовий** методи технічного замикання, а за режимом замикання - статичний і динамічний. Методи **частотного** скремблювання, реалізовані на елементах аналогової техніки, з'явилися раніше, ніж тимчасові методи, які набагато легше виконувати на елементах дискретної техніки.

Найпростішими способами є інверсії частоти та часу. У скремблері, який виконує інверсію спектру, спектр мовного сигналу обертається навколо деякої центральної частоти. Алгоритм перетворення спектру може бути ускладнений у скремблері шляхом передачі частини мовного сигналу без інверсії та з інверсією.

У скремблері, який виконує частотні перестановки, спектр вихідного мовного сигналу розбивається на кілька частотних смуг однакової або неоднакової ширини. Їх змішування виконується за певним алгоритмом (ключем). При прийомі сигналу спектр відновлюється в результаті зворотних процедур.

Інші типи трансформацій носіїв мовної інформації реалізують тимчасові методи технічного закриття з вищим рівнем захисту інформації. **Інверсія кадру** забезпечується попереднім збереженням в пам'яті передавального скремблеру сегменту голосового повідомлення (кадру) з тривалістю **Tk** і зчитування його з кінця кадру - інверсно. Після отримання кадр голосового повідомлення зберігається і зчитується з пристрою пам'яті в зворотному порядку, що відновлює вихідне повідомлення. Щоб досягти незрозумілості мови, тривалість кадру повинна бути не менше 250 мс. При цьому загальна тривалість запам’ятовування та зворотної передачі кадру становить приблизно 500 мс, що може створити значні затримки сигналу під час телефонної розмови. У процесі технічного закриття з тимчасовою перестановкою кадр голосового повідомлення розбивається на сегменти кожної тривалості. Послідовність передачі сегментів у лінії визначається за допомогою ключа, який повинен бути відомий стороні, що приймає.

Змінюючи ключ під час сеансу зв’язку в скремблерах з динамічним закриттям, можна значно підвищити рівень захисту мовної інформації. Залишкова розбірливість залежить від тривалості кадру і зменшується зі збільшенням останнього.

12.2. Засоби контролю телефонних ліній

Як ми згадували раніше сигнали поширюються по лініях зв'язку в аналоговому та цифровому вигляді. В результаті несанкціонованого перехоплення цих сигналів і їх модуляції мовна інформація може бути здобута зловмисником.

При захисті телефонних апаратів і телефонних ліній необхідно враховувати кілька аспектів:

- Телефонні апарати можуть бути використані для перехоплення акустичної мовної інформації з приміщень, в яких вони встановлені;
- Телефонні лінії, що проходять через приміщення, можуть використовуватися як джерела живлення акустичних закладок, встановлених в цих приміщеннях, а також для передачі перехопленої інформації;
- І, звичайно, може бути здійснено перехоплення телефонних розмов шляхом гальванічного або через індукційний датчик підключення до телефонної лінії закладок, диктофонів і інших засобів несанкціонованого знімання інформації.

Телефонний апарат має декілька елементів, що мають здатність перетворювати акустичні коливання в електричні, тобто володіють **"мікрофонним ефектом".** До них відносяться: ланцюг дзвінка, телефонний і мікрофонний динамік. За рахунок електроакустичних перетворень в цих елементах виникають інформаційні сигнали.

При використанні для знімання інформації методу **"Високочастотного нав'язування"**, не дивлячись на гальванічне відключення мікрофону від телефонної лінії, сигнал нав'язування завдяки високій частоті проходить в мікрофонний ланцюг і модулюється по амплітуді інформаційним сигналом.

Отже, в телефонному апараті необхідно захищати як ланцюг дзвінка, так і ланцюг мікрофону. Для захисту телефонного апарата від витоку акустичної (мовної) інформації по електроакустичних каналу використовуються як пасивні, так і активні методи і засоби.

До найбільш широко застосовуваним пасивним методам захисту відносяться:

- обмеження небезпечних сигналів;
- фільтрація небезпечних сигналів;
- відключення перетворювачів (джерел) небезпечних сигналів.

Можливість обмеження небезпечних сигналів ґрунтується на нелінійних властивостях напівпровідникових елементів, головним чином діодів. У схемі обмежувача малих амплітуд використовуються два зустрічно-включених діода. Такі діоди мають великий опір для струмів малої амплітуди і одиниці Ом і менше - для струмів великої амплітуди (корисних сигналів), що виключає проходження небезпечних сигналів малої амплітуди в телефонну лінію і практично не впливає на проходження через діоди корисних сигналів. Діодні обмежувачі включаються послідовно в лінію дзвінка або безпосередньо в кожну з телефонних ліній.

Фільтрація небезпечних сигналів використовується головним чином для захисту телефонних апаратів від **"Високочастотного нав'язування"**. Найпростішим фільтром є конденсатор, встановлюваний в ланцюг дзвінка телефонних апаратів з електромеханічним дзвінком і в мікрофонний ланцюг всіх апаратів. Ємність конденсаторів вибирається такої величини, щоб зашунтувати зондувальні сигнали високочастотного нав'язування і не робити істотного впливу на корисні сигнали. Зазвичай для установки в ланцюг дзвінка використовуються конденсатори ємністю 1 мкФ, а для установки в мікрофонний ланцюг - місткістю 0,01 мкФ. Більш складний фільтруючий пристрій є багатоланковим фільтром низької частоти на LC-елементах.

Активні методи захисту від витоку інформації по електроакустичних каналу передбачають лінійне зашумлення телефонних ліній. Шумовий сигнал подається в лінію в режимі, коли телефонний апарат не використовується (трубка встановлена). При знятті трубки телефонного апарату подача в лінію шумового сигналу припиняється.

Для захисту акустичної інформації в виділених приміщеннях поряд із захистом телефонних апаратів необхідно вживати заходів і для захисту безпосередньо телефонних ліній, так як вони можуть використовуватися як джерела живлення акустичних закладок, встановлених в приміщеннях, а також для передачі інформації, одержуваної цими закладками. Захист телефонних розмов від перехоплення здійснюється головним чином активними методами. До основних з них відносяться:

- Подача під час розмови в телефонну лінію синфазного маскуючого низькочастотного сигналу (метод синфазного низькочастотного маскування);
- Подача під час розмови в телефонну лінію маскуючого високочастотного сигналу звукового діапазону (метод високочастотного маскування);
- Подача під час розмови в телефонну лінію маскуючого високочастотного ультразвукового сигналу (метод ультразвукового маскування);
- Підняття напруги в телефонній лінії під час розмови (метод підвищення напруги);
- Подача під час розмови в лінію напруги, що компенсує постійну складову телефонного сигналу (метод «обнулення»);
- Подача в лінію при встановленій телефонній трубці маскуючого низькочастотного сигналу (метод низькочастотного маскування);
- Подача в лінію при прийомі повідомлень маскуючого низькочастотного (мовного діапазону) з відомим спектром (компенсаційний метод);

- Подача в телефонну лінію високовольтних імпульсів (метод «випалювання»).

Суть методу синфазного маскування низькочастотної (НЧ) перешкоди полягає в подачі в кожен провід телефонної лінії з використанням єдиної системи заземлення апаратури АТС і нульового проводу електромережі 220 В (нульовий провід електромережі заземлений) узгоджених за амплітудою і фазі маскуючих сигналів мовного діапазону частот (як правило, основна потужність перешкоди зосереджена в діапазоні частот стандартного телефонного каналу: 300 ... 3400 гц). У телефоні ці завадні сигнали компенсують один одного і не заважають корисному сигналу (телефонній розмові). Якщо інформація знята з одного проводу телефонної лінії, сигнал перешкод не компенсується. А оскільки його рівень набагато вище корисного сигналу, то перехоплення інформації (виділення корисного сигналу) стає неможливим. Як маскуючий (перешкоджаючий) сигнал, як правило, використовуються дискретні сигнали (псевдовипадкові послідовності імпульсів).

Метод синфазного маскуючого низькочастотного сигналу використовується для придушення телефонних радіо-закладок (як з параметричною, так і з кварцовою стабілізацією частоти) з послідовним (в розрив одного з проводів) включенням, а також телефонних радіо-закладок і диктофонів з підключенням до лінії (до одного з дротів) за допомогою індукційних датчиків різного типу .

Метод високочастотного маскування перешкоди полягає в подачі під час розмови в телефонну лінію широкосмугового маскуючого сигналу в діапазоні високих частот звукового діапазону. Даний метод використовується для придушення практично всіх типів підслуховуючих пристроїв як контактного (паралельного і послідовного) підключення до лінії, так і при підключенні з використанням індукційних датчиків. Однак ефективність придушення засобів знімання інформації з підключенням до лінії за допомогою індукційних датчиків значно нижче, ніж засобів з гальванічним підключенням до лінії. Як маскуючий сигнал використовуються широкосмугові аналогові сигнали типу "білого шуму" або дискретні сигнали типу псевдовипадкової послідовності імпульсів.

Частоти маскуючих сигналів підбираються таким чином, щоб після проходження селективних ланцюгів модулятора закладки або мікрофонного підсилювача диктофона їх рівень виявився достатнім для придушення корисного сигналу (мовного сигналу в телефонній лінії під час розмов абонентів), але в той же час ці сигнали погіршували якість телефонних розмов . Чим нижче частота шумового сигналу, тим вище його ефективність і тим більше він заважає отримати доступ до корисного сигналу. Зазвичай використовуються частоти в діапазоні від 6 ... 8 кГц до 16 ... 20 кГц. Такі маскуючі перешкоди викликають значні зменшення відношення сигнал / шум і спотворення корисних сигналів (погіршення розбірливості мови) при перехопленні їх всіма типами підслуховуючих пристроїв. Крім того, у радіо-закладок з параметричної стабілізацією частоти ("м'яким" каналом) як послідовного, так і паралельного включення спостерігається «відхід» несучої частоти, що може привести до втрати каналу прийому.

Для виключення впливу маскуючого сигналу на телефонну розмову в пристрої захисту встановлюється спеціальний низькочастотний фільтр з граничною частотою 3,4 кГц, що пригнічує (шунтує) перешкоджаючі сигнали і не робить істотного впливу на проходження корисних сигналів. Аналогічну роль виконують смугові фільтри, встановлені на міських АТС, що пропускають сигнали, частоти яких

відповідають стандартному телефонному каналу (300 Гц ... 3,4 кГц), і пригнічують шумовий сигнал.

Метод ультразвукової маскує перешкоди в основному аналогічний розглянутому вище. Відмінність полягає в тому, що використовуються перешкоджаючі сигнали ультразвукового діапазону з частотами від 20 ... 25 кГц до 50 ... 100 кГц.

Метод підвищення напруги полягає в піднятті напруги в телефонній лінії під час розмови і використовується для погіршення якості функціонування телефонних радіо-закладок. Підняття напруги в лінії до 18 ... 24 В викликає у радіо-закладок з послідовним підключенням і параметричною стабілізацією частоти «відхід» несучої частоти і погіршення розбірливості мови унаслідок розмиття спектру сигналу. У радіо-закладок з послідовним підключенням і кварцовою стабілізацією частоти спостерігається зменшення відношення сигнал / шум на 3 ... 10 дБ.

Метод «обнулення» передбачає подачу під час розмови в лінію постійної напруги, відповідної напрузі в лінії при піднятій телефонній трубці, але зворотної полярності.

Метод низькочастотного маскування полягає в подачі в лінію при встановленій телефонній трубці маскуючого сигналу мовного діапазону частот і застосовується для придушення дротових мікрофонних систем, що використовують телефонну лінію для передачі інформації на низькій частоті, а також для активізації (включення на запис) диктофонів, що підключаються до телефонної лінії за допомогою адаптерів або індукційних датчиків, що призводить до змотування плівки в режимі запису шуму (тобто за відсутності корисного сигналу).

Компенсаційний метод використовується для одностороннього маскування (приховування) мовних повідомлень, переданих абоненту по телефонній лінії. Суть методу полягає в наступному. При передачі приховуваного повідомлення на приймальній стороні в телефонну лінію за допомогою спеціального генератора подається маскуючий шум. Одночасно цей же маскуючий сигнал ("чистий" шум) подається на один із входів двоканального адаптивного фільтра, на інший вхід якого надходить адитивна суміш корисного сигналу мовного сигналу і цього ж шумового сигналу. Адитивний фільтр компенсує шумову складову і виділяє корисний сигнал, який подається на телефонний апарат або пристрій звукозапису.

Недоліком даного методу є те, що маскування мовних повідомлень одностороннє і не дозволяє вести двосторонні телефонні розмови.

Метод "випалювання" реалізується шляхом подачі в лінію високовольтних (напругою понад 1500 В) імпульсів, що приводять до електричного "випалюванню" вхідних каскадів електронних пристроїв перехоплення інформації і блоків їх живлення, гальванічно підключених до телефонної лінії. При використанні даного методу телефонний апарат від лінії відключається. Подача імпульсів в лінію здійснюється двічі. Перший (для "випалювання" паралельно підключених пристроїв) - при розімкнутої телефонної лінії, другий (для "випалювання" послідовно підключених пристроїв) - при закороченому телефонній лінії.

Для захисту телефонних ліній використовуються як прості пристрої, що реалізують один метод захисту, так і складні, що забезпечують комплексний захист ліній різними методами, включаючи захист від витоку інформації по електроакустичних каналах.

Методи контролю телефонних ліній в основному засновані на тому, що будь-яке підключення до них викликає зміну електричних параметрів ліній: амплітуд напруги і струму в лінії, а також значень ємності, індуктивності, активного і реактивного опору лінії.

Простий пристрій контролю телефонних ліній являє собою вимірювач напруги. При налаштуванні оператор фіксує значення напруги, відповідне нормальному стані лінії, і поріг «тривоги». При зменшенні напруги в лінії більш встановленого порога пристроєм подається світловий або звуковий сигнал тривоги.

На принципах вимірювання напруги в лінії побудовані і пристрої, які сигналізують про розмикання телефонної лінії, яка виникає при послідовному підключенні закладного пристрою.

Як правило, подібні пристрої містять також фільтри для захисту від прослуховування за рахунок "мікрофонного ефекту" в елементах телефонного апарату і високочастотного "нав'язування". Пристрої контролю телефонних ліній, побудовані на розглянутому принципі, реагують на зміни напруги, викликані не тільки підключенням до лінії засобів знімання інформації, але і коливаннями напруги на АТС (що для вітчизняних ліній досить часте явище), що призводить до частих помилкових спрацьовувань сигнальних пристроїв. Крім того, ці пристрої не дозволяють виявити паралельне підключення до лінії високоомних підслуховуючих пристроїв. Тому подібні пристрої не знаходять широкого застосування на практиці.

Принцип роботи більш складних пристроїв заснований на періодичному вимірі і аналізі декількох параметрів лінії. Такі пристрої дозволяють визначити не тільки факт підключення до лінії засобів знімання інформації, але і спосіб підключення (послідовне або паралельне). Наприклад, контролери телефонних ліній "КТЛ-2", "КТЛ-3" і "КТЛ-400" за 4 хвилини дозволяють виявити закладки з живленням від телефонної лінії незалежно від способу, місця та часу їх підключення, а також параметрів лінії і напруги АТС . Прилади також видають світловий сигнал тривоги при короткочасному (не менше 2 секунд) розмиканні лінії.

Сучасні контролери телефонних ліній, як правило, поряд із засобами виявлення підключення до лінії пристроїв несанкціонованого знімання інформації, обладнані і засобами їх придушення. Для придушення в основному використовується метод високочастотної маскує перешкоди та включається автоматично або оператором при виявленні факту несанкціонованого підключення до лінії. Для блокування роботи несанкціоновано підключених паралельних телефонних апаратів використовуються спеціальні електронні блокіратори.

Принцип роботи подібних пристроїв полягає в наступному. У черговому режимі пристрій захисту робить аналіз стану телефонної лінії шляхом порівняння напруги в лінії і на еталонній навантаженні, підключеної до ланцюга телефонного апарату. При піднятті трубки несанкціоновано підключеного паралельного телефонного апарата напруга зменшується, що фіксується пристроєм захисту. Якщо цей факт зафіксований в момент ведення телефонної розмови спрацьовує звукова і світлова сигналізація. А якщо факт несанкціонованого підключення зафіксований у відсутності телефонної розмови, то спрацьовує сигналізація і пристрій захисту переходить в режим блокування набору номера з паралельного телефонного апарата. У цьому режимі пристрій захисту шунтує телефонну лінію опором 600 Ом, що виключає можливість набору номера з паралельного телефонного апарата.

Крім несанкціонованого підключення до лінії паралельного телефонного апарата подібні пристрої сигналізують також про факти обриву (розмикання) і короткого замикання телефонної лінії. Найефективнішим способом захисту телефонних повідомлень від несанкціонованого доступу є їх криптографічне перетворення.

Для того, щоб приховати від зловмисників смисловий зміст переданого телефонного повідомлення, його необхідно певним чином змінити. При цьому змінити його так, щоб відновлення вихідного повідомлення санкціонованим абонентом здійснювалося б дуже просто, а відновлення повідомлення зловмисником було б неможливим або вимагало б істотних тимчасових і матеріальних витрат, що робило б сам процес відновлення неефективним.

12.3. Перехват повідомлень в GSM каналах

На сьогоднішній день Глобальна система мобільного зв'язку (GSM – Global System for Mobile Communications) найбільш розповсюджена і зручна система зв’язку, але вважається застарілою, і багато хто відмовляться неї, вибираючи більш сучасних, таких як Універсальна система мобільного зв'язку (UMTS - універсальна мобільна телекомунікаційна система) та LTE (Long Term Evolution). Безпека GSM забезпечується, набором алгоритмів, які використовуються для організації з'єднання стільникового телефону з мережею оператора (рис. 12.3).

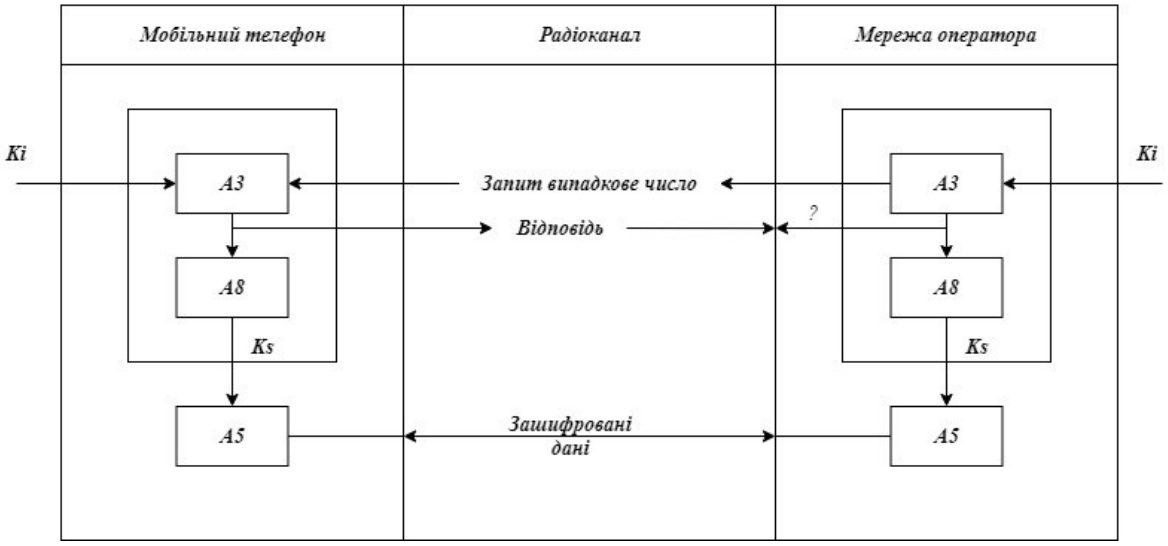

Рисунок 12.3 - Алгоритм з'єднання стільникового телефону з мережею оператора GSM

Основу безпеки GSM складають три закритих алгоритми:

- A3 – алгоритм, який використовується для аутентифікації;
- A8 – алгоритм, за допомогою якого генерується ключ шифрування для одного сеансу зв'язку;
- A5 – алгоритм, шифрування сигналу під час сеансу зв'язку.

Кожен стільниковий телефон стандарту GSM обладнаний модулем ідентифікації абонента SIM-картою (SIM - Subscriber Identification Module), на якій міститься інформація, яка унікальним чином ідентифікує стільниковий телефон в мережі - міжнародний ідентифікатор мобільного абонента (IMSI - International

Mobile Subscriber Identity).

Аутентифікація користувача (можливість однозначно визначити, хто підключився до мережі) заснована на методі "запит-відповідь". Мережа GSM надсилає запит на стільниковий телефон, в якому міститься певна випадкове число. Телефон шифрує його з допомогою аутентификаційного алгоритму A3, використовуючи ключ шифрування Ki які знаходяться на SIM-карті.

Основна завдача алгоритму - генерація відклику (SRES – Signed Response) на випадковий пароль, одержуваний стільниковим телефоном (MS) від центру комутації (MSC) в процедурі аутентифікації. Суть аутентифікації в GSM - уникнути клонування мобільного телефону користувача. Криптозахист в мережі GSM є криптографічною системою з відкритим ключем. Секретний 128-бітний ключ Ki, яким володіє як абонент, так і центр аутентифікації (AuC). Також в аутентифікації беруть участь домашній реєстр місцеположення (HLR) і центр комутації (MSC).

Коли MS запитує доступ до мережі, MSC повинен перевірити справжність MS. Для цього MSC відправляє в HLR унікальний міжнародний ідентифікатор абонента (IMSI) і запит на отримання набору спеціальних триплетів. Коли HLR отримує IMSI запит на триплети, він спочатку перевіряє свою базу даних, щоб упевнитися, що MS з таким IMSI дійсно належить мережі. Якщо перевірка пройшла успішно, то HLR відправляє IMSI і запит встановлення автентичності в AuC. Який використовує IMSI, щоб знайти Ki що від-повідає цьому IMSI. Також AuC генерує випадкове 128-бітове число RAND. Після цього AuC обчислює 32-бітний відгук SRAND (SRAND - Signed Response) за допомогою алгоритму A3: SRAND = A3 (RAND, Ki). Крім то-го, AuC обчислює 64-бітний сеансовий ключ Kc за допомогою алгоритму A8:

Kc = A8 (RAND, Ki).

Kc надалі використовується в алгоритмі A5 для шифрування і розшифрування даних. RAND, SRES, і Kc утворюють три-плети, які MSC запросив у HLR. AuC генерує п'ять таких триплетів і посилає їх в HLR, потім HLR пересилає цей набір в MSC. Набір триплетів генерується для того, щоб зменшити передачу сигналів в NSS , яка відбувалася б кожен раз, коли MS запитувала б доступ до мережі, а MSC мав би перевірити справжність MS. Слід зазначити, що набір триплетів унікальний для одного IMSI і не може бути використаний для будь-якого іншого IMSI.

IMSI-пастки - це мобільні неправдиві базові станції, які спецслужби включають при різних обставинах в різних місцях. Мобільні телефони "чіпляються" до цих станцій, які фактично виступають в ролі Man-in-the-middle. Воно може підтримувати 2 режиму - активний і пасивний. В активному пастка виступає в ролі базової станції. У пасивному - моніторить канал і інші базові станції.

Існує кілька режимів:

- A5 / 0 - фактично це plain text, шифрування немає;
- A5 / 1 - перший варіант з потоковим шифром, який зараз вже не вважається досить стійким;
- A5 / 2 - експортний варіант A5 / 1 з навмисно заниженою стійкістю;
- A5 / 3 - досить стійкий варіант, який виник з приходом 3G.

Як показав відомий хакер Harald Welte , вся схема захисту в GSM місцями ґрунтується на популярному принципі Security through obscurity і містить фундаментальні уразливості. Якщо оператор спочатку всюди застосовує A5 / 2, то завдання стає очевидною - цей шифр розкривається в реальному часі. Але оператори

використовують A5 / 1. Базова станція анонсує цей протокол і телефон на нього "погоджується", всі задоволені. Всі шифри A5 працюють на ключі, який зберігається як у оператора, так і на SIM-карті. Він унікальний для кожного абонента і за його збереження відповідає кріпточіп SIM-карти. З цього випливає, що пастка по відношенню до оригінальної базової станції "прикидається" абонентським пристроєм на алгоритмі A5 / 1, а для реального телефону "прикидається" базовою станцією на алгоритмі A5 / 2, який розкривається на льоту. Таким чином, пастка витягує секретний ключ абонента і реконструює сесію з базовою станцією. Справу зроблено. Як дізнатися, що ваш телефон переключився на слабкий шифр? Зазвичай ніяк: індустрія стільникового зв'язку піклується про людей - менше знаєш, краще спиш. Однак в природі все ж зустрічаються окремі моделі телефонів, які якось сигналізують, і це не смартфони. Десь з'являється іконка, а десь непомітна рядок витікає в лог, однак це зазвичай пов'язане з переходом на A5 / 0.

13. МЕТОДИ І ЗАСОБИ ТЕХНІЧНОЇ ОХОРОНИ ОБ’ЄКТІВ. СИСТЕМИ СИГНАЛІЗАЦІЇ ТА ВІДЕО СПОСТЕРЕЖЕННЯ

1. Системи телевізійного спостереження.
2. Засоби телевізійної охорони.
3. Основні характеристики відеокамер.
4. Засоби запису та реєстрації зображення.
5. Класифікація систем відеоспостереження.

13.1. Системи телевізійного спостереження

Найбільш проста система телевізійного спостереження включає телевізійну камеру й монітор. Камера може бути підключена безпосередньо до телевізора або монітора. При цьому ви можете, наприклад, спостерігати за своєю дитиною, що грає в сусідній кімнаті, автомобілем біля будинку та ін. Для невеликого об’єкта охорони досить не більше чотирьох-п’яти камер. Використовуючи монітор з вбудованим комутатором і вдало розташувавши камери, можна забезпечите цілодобове спостереження за контрольованою територією.

Камери можуть розташовуватися усередині приміщення на поворотних пристроях. При цьому в денний час вони можуть використовуватися для контролю в торговельному залі, а ввечері й уночі – для контролю охоронюваної території. Кількість одночасно відображуваних камер повинне бути обмежено. При збільшенні кількості моніторів операторові важко стежити за всіма змінами. У багатокамерних системах використовуються додаткові пристрої До додаткових пристроїв ставляться детектори руху, які аналізують зміни зображення, наприклад, переміщення будь-якого предмета в поле зору камери й сигналізують операторові про цьому. Для дистанційного керування камерами використовуються поворотні пристрої. Вони дозволяють збільшити огляд камери за допомогою її повороту у двох площинах. Керування поворотними пристроями може здійснюватися джойстиком.

13.2. Засоби телевізійної охорони

На об'єктах, що охороняються підрозділами охорони, можуть використовуватися тільки пристрої ТСВ, що мають сертифікати відповідності: - телекамери, - пристрої керування режимом відображення, - монітори, - комп'ютери, - спеціалізовані охоронні

відеомагнітофони, - джерела живлення, - поворотні пристрої. На об'єктах, що охороняються підрозділами охорони, можуть використовуватися тільки ТСВ, які відповідають наступним стандартам: для систем кольорового телебачення - стандарту PAL, для систем чорно-білого - CCIR. Застосування пристроїв ТСВ інших стандартів можливе лише у тих випадках, коли необхідна додаткова установка пристроїв ТСВ на об'єктах, що охороняються, де вже експлуатуються пристрої ТСВ інших стандартів. Побудова ТСВ має здійснюватися за модульним принципом. За функціональними ознаками системи відеоспостереження поділяють на наступні модулі: - модулі відеоспостереження; - модулі відеозапису; - модулі відеоохрани; - модулі відеопередачі по кабельних і провідним мережам; модулі відеопередачі по бездротових каналах зв'язку; - модулі відеопередачі по цифрових каналах і комутованих лініях загального користування. Вибір пристроїв ТСВ для використання в модулях вищого класу для застосування на особливо важливих об'єктах, у тому числі для охорони установ банків, здійснюється з урахуванням наступних вимог: - Допускається застосування кольорових телекамер із чутливістю не гірше 4 лк на ПЗС-матриці. - При необхідності забезпечення змінного кута огляду зони, що охороняється допускається застосування трансфокатором і поворотних пристроїв. - Телекамери для внутрішнього і зовнішнього спостереження в залежності від умов експлуатації можуть забезпечуватися інфрачервоним підсвічуванням. - Пристрої обробки відеозображення (комутатори, квадратори, мультиплексори, матричні комутатори) вибираються в залежності від конкретної конфігурації системи відеоспостереження, тобто кількості телекамер (відеовходів) і пристроїв контролю (відеовиходів), завдань охорони та вимог до якості відеозапису та зображення, що виводиться на екран монітора. - Для контролю зображення в повноекранному режимі повинні використовуватися монітори 5 "(13 см), 9" (23 см), 12 "(31 см), для перегляду мультікартіни (одночасне виведення зображення від декількох телекамер) - монітори 14" (35 см) , 15 "(38 см), 17" (43 см), 20 "(50 см), 21" (51 см), 28 "(70 см). - Дозвіл чорно-білих моніторів по горизонталі, застосовуваних у системах відеоспостереження установ банків, повинно бути не менше 700 телевізійних ліній в центрі екрану. - При використанні кольорових телевізійних камер допускається застосовувати кольорові монітори з роздільною здатністю по горизонталі не менше 340 телевізійних ліній в центрі екрану. - Всі модулі ТСВ для установки в установах банків повинні в обов'язковому порядку комплектуватися спеціалізованими охоронними магнітофонами класу S - VHS. - Записана на відеокасеті інформація повинна зберігатися не менше 7 діб. - Для запису зображення повинні використовуватися спеціалізовані охоронні відеомагнітофони, дозволяють записувати зображення контрольованого об'єкта, що отримується з однієї або декількох камер в реальному часі або покадровому режимі з різними часовими проміжками (паузами) між окремими - Спецвідеомагнітофон повинен мати відповідні входи і можливість при надходженні сигналу тривоги від засобів охоронної, тривожної сигналізації або систем контролю доступу переходу на запис в режимі реального часу. - Все обладнання, обране для системи відеоспостереження, повинно бути одного стандарту. - Для виключення впливу зовнішніх кліматичних умов на відеокамеру необхідно застосовувати спеціальні кліматичні кожухи. - Для захисту відеокамери від механічних пошкоджень (ударів) необхідно застосовувати спеціальні кожухи, виготовлені з високоміцних матеріалів(сплавів) і скла.

13.3. Основні характеристики відеокамер

У сучасних камерах відеоспостереження в якості перетворювача світла в електричний сигнал застосовуються прилади з позарядовой записом (ПЗС), що становлять основу ПЗС-матриць. На сьогоднішній день більшість відеокамер проводиться на основі матриць Sony, Panasonic, Sharp, LG, Samsung. Формат матриці (дюйм) - розмір діагоналі матриці в дюймах, що визначає кут зору при використанні об'єктива с тим чи іншим фокусною відстанню. Найбільш поширені камери відеоспостереження з форматами 1/2 ", 1/3", 1/4 ". Чим більше формат матриці, тим більше розміри камери, причому розміри матриці жодним чином не впливають на показники якості зображення. Дозвіл (ТВЛ) - параметр, що характеризує детальність зображення, одним словом, чим більше дозвіл, чим краще проглядаються дрібні деталі, такі як номер автомобіля, особа людини. Вимірюється в телевізійних лініях (ТВЛ), причому мається на увазі роздільна здатність по горизонталі, так як дозвіл по вертикалі у відеокамер одного стандарту однаково і обмежена на одному рівні (400 ТВЛ для стандарту CCIR / PAL і 330 ТВЛ для EIA / NTSC). Чорно-білі камери відеоспостереження стандартного дозволу мають дозвіл 380-420 ТВЛ, підвищеного дозволу 560-570 ТВЛ, кольорові камери 280-350 ТВЛ, з високою роздільною здатністю до 460 ТВЛ, а з цифровою обробкою відеосигналу (DSP) до 560 ТВЛ по S-VHS виходу . Чутливість (люкс) - мінімальний рівень освітленості (в люксах), при якому камера відеоспостереження дає розпізнається відеосигнал. Це найбільш заплутаний параметр, оскільки не існує чіткого визначення. Найбільш частіше під чутливістю розуміють мінімальну освітленість на об'єкті, що вимірюється при світлосилі об'єктива 1,4. Для звичайних чорно-білих камер вона становить 0,4 ~ 0,01 люкс (сутінки), для високочутливих до 0,00015 люкс (темна ніч), для кольорових 0,2 ~ 3 люкс. Іноді виробники вказують мінімальну освітленість на матриці, яка в 10 разів вище Варто згадати, що чутливість чорно-білих відеокамер зачіпає не тільки спектр видимого світла, але інфрачервону область, що дозволяє застосовувати ІК-підсвічування в умовах низької освітленості. Відношення сигнал-шум (дБ) - виражає співвідношення амплітуд відеосигналу і шуму в логарифмічною шкалою. S / N = 20 log (відеосигнал / шум). Одним словом S / N = 50 дБ говорить про те, що амплітуда відеосигналу більше амплітуди шуму в 316 разів. Це дозволяє спостерігати чітку картинку, при значенні S / N = 40 дБ помітні дрібні перешкоди, особливо в умовах низької освітленості. При S / N = 20 дБ на екрані вже буде суцільна «брижі». Електронний затвор (сек) - іншим словом час експозиції матриці, що забезпечує середню яскравість зображення в динамічно змінною світловий обстановці. Це досягається за рахунок часу накопичення заряду в осередках ПЗС-матриці, яке при яскравому освітленні може досягати 1/100000 сек, таким чином, імітуючи автодіафрагму об'єктива. Напруга живлення відеокамер зазвичай становить 12В постійного струму, або 24 / 220В змінного. Синхронізація камер відеоспостереження буває 3-х типів. У більшості випадків застосовується внутрішня кварцова синхронізація. У деяких випадках в камерах, що живлять змінним струмом використовується синхронізація Linelock, а живлять постійною напругою - зовнішня синхронізація. Компенсація заднього світла (BLC) - апаратна функція, що дозволяє спостерігати за об'єктом, що знаходиться на тлі яскравого світла. Цифрова обробка відеосигналу (DSP) в камерах відеоспостереження дозволяє значно розширити динамічний діапазон, застосовувати детектор руху, здійснювати перемикання режиму «день-ніч», чорно-білого і кольорового режиму, застосувати функцію PTZ.

13.4. Засоби запису та реєстрації зображення

Реєстрація зображень (зіставлення, накладання) — це процес трансформування різних наборів даних в одну координатну систему. Даними можуть бути серія фотографій, дані з різних сенсорів, моментів часу, глибини, або точок спостереження. Алгоритми реєстрації зображень використовуються в комп'ютерному баченні, методах медичної візуалізації, у військовій справі для автоматичного розпізнавання цілей, і для впорядковування і аналізу зображень із супутникових даних. Реєстрація необхідна для того, мати можливість порівнювати або інтегрувати отримані з цих різних пристроїв реєстрації даних.

Порівняння методів основаних на аналізі інтенсивності або основі виділення ознак В даному процесі, одна частина зображень являє собою опорне зображення або еталон, а інші відповідні зображення називаються цільовими, або тими, що підлягають скануванню, пошуку об'єктів. Реєстрація зображення досягається шляхом співставлення цільових зображень, так щоб вони збігалися з еталонним зображенням. У методах, що працюють з інтенсивністю зображень, порівнюють зразки інтенсивності зображення на основі кореляції показників, а в методах основаних на виділенні ознак шукають відповідності між елементами зображення, такими як точки, лінії і контури.

Алгоритми співставлення зображень також можна класифікувати відповідно до моделей трансформації, які вони використовують для співвідношення простору цільового зображення в простір еталонного зображення. Перша широка категорія моделей трансформації включає в себе лінійні відображення такі як: обертання, масштабування, переміщення і інші афінні перетворення.

Просторові методи мають справу з простором зображення порівнюючи зразки інтенсивності або елементи зображення. Деякі алгоритми виділення ознак походять від традиційних технік для виконання ручного співставлення зображень, в яких оператор вручну виділяє відповідні контрольні точки в зображеннях. Коли кількість контрольних точок перевищує мінімум, що необхідний для визначення правильної моделі трансформації, можуть застосовуватись ітеративні алгоритми, щоб швидко оцінити параметри конкретного типу перетворення для співставлення зображень.

Одномодальні методи намагаються реєструвати зображення отримані в одному режимі за допомогою однакового типу сенсора/сканера, в той час як мультимодальні методи реєстрації працюють з зображеннями, що отримані з різних типів і режимів роботи сенсорів.

Методи реєстрації можна класифікувати відносно рівня автоматизації, що вони забезпечують. Існують ручні, інтерактивні, полу-автоматичні і автоматичні методи. Ручні методи надають інструменти для зіставлення зображень вручну. Інтерактивні методи дозволяють зменшити систематичні помилки користувача, виконуючи певні ключові операції автоматично, але потребують участі користувача для контролю процесу реєстрацію.

Міри схожості зображень визначають ступінь схожості між образами інтенсивності двох зображень. Вибір міри схожості зображення залежить від модальності зображень, які зіставляються. Типовими прикладами таких мір схожості зображень є крос-кореляція, взаємна інформація, сума квадратів різниць інтенсивності, і співвідношення однорідності зображення. Міра взаємної інформації і нормалізованої взаємної інформації є найбільш популярною мірою схожості при

співставленні мультимодальних зображень. Невизначеність Існує рівень невизначеності, що пов'язана з реєстрацією зображень, які мають які-небудь просторово-часові відмінності. Реєстрація зображень з мірою невизначеності є необхідною для багатьох застосувань виявлення змін, таких як медична діагностика.

В задачах дистанційного спостереження в яких цифрове зображення може представляти кілька кілометрів просторової відстані, невизначеність в реєстрації зображень може означати, що результат може мати деталізацію в декілька кілометрів в порівняні з точністю на поверхні землі.

13.5. Класифікація систем відеоспостереження

Комплексний захист власного житла неможливий без оперативного реагування на проникнення ззовні. Умови експлуатації в приватному будинку задають основні параметри використовуваних відеокамер і моніторів :

1) Естетичність. Це найбільш важливий критерій при вибиранні засобів спостереження за власним будинком. Останнім часом з'явилася безліч цифрових безпровідних рішень, що дозволяють істотно підвищити скритність і зручність розміщення системи відеоспостереження в будинках різної конфігурації.

2) Компактність. Відноситься до робочого місця оператора. Оператор відеоспостереження може своєчасно реагувати на події, що відбуваються.

3) Доступність. Завдяки розвитку цифрових технологій, для приватного використання сталі доступні системи відеоспостереження з високим розділенням і можливістю зйомки в нічний час.

Особливий вид систем контролю, в яких важлива як якісна картинка, так і звук. В деяких випадках може знадобитися приховане відеоспостереження для контролю над діями співробітників в робочий час. Такі системи відеоспостереження стануть ефективним способом стимулювати якість роботи. Цей ефективний метод огляду прилеглої території, реєстрації людей, що проходять, і проїжджаючих автомобілів може стати частиною комплексної системи безпеки будівлі будь-якої складності. Сучасні відеореєстратори дозволяють не лише розпізнавати номери машин і обличчя людей, але і автоматично порівнювати їх з наявними в базі даних. Результатом такого порівняння може бути відкриття шлагбауму або навпаки, виклик охорони.

Як правило, для великої системи відеоспостереження на перший план виходять наступні характеристики: a) Функціональність; b) Універсальність; c) Всепогодність; d) Можливість роботи в темний час доби.

Усім цим вимогам задовольняють цифрові камери з інфрачервоним підсвічуванням нового покоління. Приховане відеоспостереження і відеоспостереження в темних місцях Для цих цілей використовуються спеціалізовані відеокамери, досить компактні, обладнані інфрачервоним підсвічуванням.

У тому випадку, якщо необхідно забезпечити автономність відеореєстраторів або їх мобільність, використовують системи відеоспостереження, що використовують для передачі даних безпровідні мережі Wi-Fi, 3G і GPRS. Це істотно спрощує монтаж комплексної системи безпеки, дозволяє розташовувати відеокамери в нестандартних місцях, забезпечуючи велику повноту огляду місцевості. Мобільні системи відеоспостереження також широко поширені на транспорті і в інтер'єрах, де прокладення додаткових кабелів недопустиме.

Підписано до друку 18.04.2023 р.
Формат 60х84/16. Папір офсетний.
Друк офсетний. Зам. № 23-10247
Умов.-друк. арк. 3,5. Обл.-вид. арк. 5,1.
Тираж 30 прим.

Віддруковано ФО-П Шпак В. Б.
Свідоцтво про державну реєстрацію В02 № 924434 від 11.12.2006 р.
м. Тернопіль, бульвар Просвіти, 6/4. тел. 097 299 38 99.
E-mail: tooums@ukr.net

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції ДК № 7599 від 10.02.2022 р.