МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____ 2022 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 «Кібербезпека»

на тему: **СИСТЕМА ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В КІМНАТІ НАРАД**

Студент групи СЗД-42 Миронюк Георгій Юрійович _____
(підпис)

Науковий керівник: к.т.н., доц. Шуклін Герман Вікторович _____
(підпис)

Нормоконтроль ст. викл. Гребенніков Асаді Болдхоягович _____
(підпис)

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н., доц. Г.В. Шуклін
«_____»_____ 2022р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Миронюку Георгію Юрійовичу

1. Тема роботи: Система забезпечення захисту інформації в кімнаті нарад

Затверджена наказом по університету від «____»_____ 2022 р. № ___

2. Термін здачі студентом оформленої роботи «____» _____ 2022 р.

3. Об'єкт дослідження: є захист інформації від витоку по акустичним та віброакустичним каналам на об'єкті інформаційної діяльності.

4. Предмет дослідження: є методи та засоби захисту акустичної інформації на об'єкті інформаційної діяльності.

5. Мета роботи: розробка системи захисту інформації від витоку по акустичному та віброакустичному каналах при проведенні нарад на об'єкті інформаційної діяльності.

6. Перелік питань, які мають бути розроблені:

1. Аналіз існуючих підходів до захисту інформації від витоку по акустичному та віброакустичному каналах.
2. Вимоги до захисту акустичної інформації на об'єкті інформаційної діяльності.
3. Засоби несанкціонованого отримання акустичної інформації.
4. Методи захисту акустичної інформації.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____2022 р.

Науковий керівник _____ Шуклін Г.В.

Завдання прийняв до виконання _____ Миронюк Г.Ю.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз існуючих підходів до захисту інформації від витоку по акустичному та віброакустичному каналах		
2	Вимоги до захисту акустичної інформації на об’єкті інформаційної діяльності		
3	Засоби несанкціонованого отримання акустичної інформації		
4	Методи захисту акустичної інформації		
5	Реферат, вступ, висновки		
6	Підготовка презентації до захисту		

Студент _____ Миронюк Г.Ю.

(підпис) (прізвище та ініціали)

Керівник бакалаврської роботи _____ Шуклін Г.В.

(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина бакалаврської роботи: 71 сторінка, 34 рисунки, 28 джерел.

Об’єкт дослідження – захист акустичної інформації на об'єкті інформаційної діяльності

Предмет дослідження – методи та засоби захисту акустичної інформації на об'єкті інформаційної діяльності.

Мета роботи – розробка системи захисту інформації від витоку по акустичному каналу.

Методи дослідження – теорія електрозв’язку, теорія інформації, системний аналіз.

У роботі приведено основні відомості про акустичний канал витоку інформації та засоби отримання акустичної інформації.

Визначені основні напрями щодо захисту акустичної інформації на об’єктах інформаційної діяльності. Проаналізовано існуючі методи захисту акустичної інформації. Проаналізовано існуючі засоби захисту акустичної інформації. На підставі проведених досліджень розроблено систему захисту акустичної інформації на об’єкті інформаційної діяльності з використанням технічних засобів.

Галузь використання – інформаційна безпека.

ГЕНЕРАТОР ВІБРОАКУСТИЧНОГО ШУМУ, ГЕНЕРАТОР ШУМУ АКУСТИЧНОГО ДІАПАЗОНУ, РАДІОЗАКЛАДКА, ЛАЗЕРНИЙ СТЕТОСКОП, АКТИВНІ ЗАХОДИ, ПАСИВІН ЗАХОДИ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВЧ – високочастотні

ДТЗС – допоміжні технічні засоби і системи

ЕМПШ – електромагнітне поле шуму

ЗІ – захист інформації

ІзОД - інформація з обмеженим доступом

НЧ – низькочастотні

ОІД – об’єкт інформаційної діяльності

ПНЧ – перетворювачі низьких частота

ПЕОМ – персональна електронно-обчислювальна машина

ПЕМІН – побічні електромагнітні випромінювання

ТЗПІ – технічні засоби приймання інформації

ВСТУП

На сучасному етапі особливою актуальною проблемою стає забезпечення захисту інформації. До 86% об’єм втрат інформації пов’язане з несанкціонованим отриманням та використанням у першу чергу це стосується тому система технічного захисту є досить важливою складовою загальної системи забезпечення охорони інформації. Захист мовної інформації є однією з найбільш важливих задач в комплексі заходів по забезпеченню інформаційної безпеки, об’єкт для перехвату мовної інформації зловмисник може використовувати широкий арсенал засобів акустичної розвідки, що дозволяють перехоплювати мовну інформації по прямому акустичному, віброакустичному, електроакустичному і оптичному (акустооптичному) каналах. Тому аналіз та дослідженням сучасних методів та засобів технічного захисту інформації має практичне значення та є актуальними.

Мета роботи – розробка системи захисту інформації від витоку по акустичному каналу.

Об’єкт дослідження – захист акустичної інформації на об'єкті інформаційної діяльності

Предмет дослідження – методи та засоби захисту акустичної інформації на об'єкті інформаційної діяльності.

Ґрунтуючись на результатах проведеного аналізу потенційних загроз і каналів витоку розроблена система захисту інформації від витоку по акустичному каналу.

Галузь застосування – інформаційна безпека.

1 АКУСТИЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

1.1. Класифікація акустичних каналів витоку інформації

Перш ніж переходити до розгляду властиво акустичних каналів витоку інформації, сформулюємо основні визначення акустики, на яких базуються відомості, наведені в данному розділі.

Звуком називаються механічні коливання часток пружного середовища (повітря, води, металу й т.д.), суб'єктивно сприймані органом слуху. Звукові відчуття викликаються коливаннями середовища, що відбуваються в діапазоні частот від 16 до 20000 Гц.

Звуковий тиск — це змінний тиск у середовищі, обумовлений поширенням у ньому звукових хвиль. Величина звукового тиску **P** оцінюється силою дії звукової хвилі на одиницю площі й виражається в ньютонах на квадратний метр (1 Н/м^2= 10 бар).

Сила (***інтенсивність***) ***звуку*** — кількість звукової енергії, що проходить за одиницю часу через одиницю площі; виміряється у ватах на квадратний метр (Вт/м^2). Слід зазначити, що звуковий тиск і сила звуку зв'язані між собою квадратичною залежністю, тобто збільшення звукового тиску в 2 рази приводить до збільшення сили звуку в 4 рази.

Рівень сили звуку — відношення сили даного звуку **I** до нульового (стандартного) рівня, за який прийнята сила звуку $\mathbf{I_0} = 10^{-12}$ Вт/м^2, виражене в децибелах (дБ)

Рівні звукового тиску й сили звуку, виражені в децибелах, збігаються по величині.

Динамічний діапазон — діапазон гучностей звуку або різниця рівнів звукового тиску найгучнішого й самого тихого звуків, виражена в децибелах.

Діапазон основних звукових частот мови лежить у межах від 70 до 1500 Гц. Однак з урахуванням обертонів мовний діапазон звучання розширюється до 5000-8000 Гц

(Рис. 1.1). В українській мові максимум динамічного діапазону перебуває в області частот 300-400 Гц (Рис. 1.2).

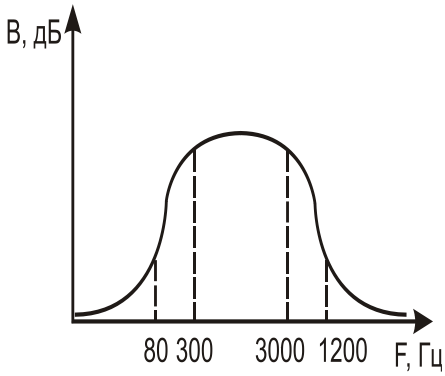

Рис. 1.1. Діапазон звучання звичайної мови

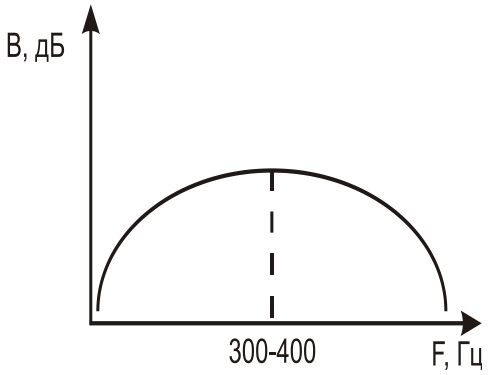

Рис.1.2.Максимум динамічного діапазону
української мови

Сприйняття людиною звуку дуже суб'єктивне. Так як всі люди сприймають звукові коливання в широких діапазонах частоти й інтенсивності. Ступінь точності, з якої людина може визначити частоту звукових коливань на слух, залежить від гостроти, та натренованості слуху.

Крім цього, чутливість людського вуха неоднакова до звукових коливань різної частоти. Основна маса людей краще розрізняє звуки в діапазоні частот від 1000 до 3000 Гц.

Така характеристика сприйманого людиною звуку, як гучність, є суб'єктивною оцінкою сили звуку. Однак гучність залежить не тільки від інтенсивності звуку (звукового тиску), але ще й від частоти.

Джерелом утворення акустичного каналу витоку інформації є вібруючі, колеблюючі тіла й механізми, такі як голосові зв'язування людини, рухливі елементи машин, телефонні апарати, звукопідсилювальні системи й т.д. Класифікація акустичних каналів витоку інформації представлена на рис. 1.3.

Рис. 1.3. Класифікація акустичних каналів

1.2. Поширення звуку в просторі

Найчастіше звук поширюється повітрям, але може поширюватися й інших середовищах. Ці середовища називають пружними. Якщо між вухом і джерелом звуку видалити звукопередавальне середовище, ми нічого не почуємо. Це означає,

що для передачі звуку на відстань необхідне звукопередавальне середовище. Пружна хвиля є поздовжньою й пов'язана з об'ємною деформацією пружного середовища, внаслідок чого може поширюватися в будь-якому середовищі - твердому, рідкому й газоподібному.

Звук є послідовністю хвиль тиску, який поширюються через середовища, що стискаються, такі як повітря або вода. (Звук може поширюватися і через тверді тіла, але є і інші способи поширення). При своєму поширенні хвилі можуть відбиватися, заломлюватися або затухати в середовищі. Мета цього експерименту - вивчити, який вплив характеристики середовища роблять на звук.

Усі середовища мають три властивості, що впливають на характер поширення звуку :

- Зв'язок між щільністю і тиском. Це співвідношення, на яке впливає температура, визначає швидкість звуку в середовищі.
- Рух самого середовища, наприклад вітри. Незалежно від руху звуку через середовище, якщо середовище рухається, звук передається далі.
- В'язкість середовища. Це визначає швидкість послаблення звуку. Для багатьох середовищ, таких як повітря або вода..

Що відбувається, коли звук поширюється в середовищі з непостійними властивостями? Наприклад, коли швидкість звуку збільшується з висотою? Звукові хвилі заломлюються. Вони можуть бути сфокусовані або розсіяні, збільшуючи або зменшуючи рівень звуку, точно так, як і оптична лінза збільшує або зменшує інтенсивність світла.

Одним із способів представлення поширення звуку є рух хвилевих фронтів - ліній постійного тиску, які переміщаються з часом. Інший спосіб - гіпотетично відмітити точку на фронті хвилі і простежити траєкторію цієї точки в часі. Цей останній підхід називається трасуванням променів і найчіткіше показує, як заломлюється звук.

У подальшому моделюванні можна візуалізувати вплив середовища на поширення звуку. Користувач може створювати різні профілі швидкості звуку і

швидкості вітру, натискаючи на варіанти профілів і перетягуючи червоні точки, щоб встановити амплітуди. Доступні два джерела звуку : сферичне джерело, в якому початкові звукові хвилі виходять рівномірно на всіх напрямках; і плоске джерело, в якому початкові звукові хвилі виходять в одному напрямі.

Розташування джерела і його орієнтацію можна змінити, перетягуючи червоні точки. Поширення звуку в цій симуляції відбувається в двох вимірах; і медіа-профілі залежать тільки від висоти. Натиснення "Старт" запустить симуляцію. Поширення представлене як променями (чорні), так і хвилевими фронтами (червоні). Зверніть увагу, що швидкість звуку C0 штучно занижена, щоб підкреслити ефекти середовища. (Номінальна швидкість звуку в повітрі складає 340 м/с, у воді - 1500 м/с.

Канал витоку мовної інформації можна розглянути у вигляді схеми, наведеної на Рис. 1.5.

Рис. 1.5. Схема каналу витоку мовної інформації

Середовища поширення мовної інформації зі способу переносу звукових хвиль діляться на:

- середовища з повітряним переносом;
- середовища з матеріальним переносом (моноліт);
- середовища з мембранним переносом (коливання скла).

Акустична класифікація приміщень здійснюється на підставі висоти **h**, ширини **b** і довжини **l** і має три групи.

Розмірні **l/h ≤ 5**.

Плоскі **l/h ≥ 5** й **b/h > 4**.

Довгі **l/h > 5** й **b/h < 4**.

Як ми вже відзначали, під акустичною розуміється інформація, носієм якої є акустичні сигнали. У тому випадку, якщо джерелом інформації є людська мова, акустичну інформацію називають *мовною*.

Первинними джерелами акустичних коливань є механічні системи, наприклад, органи мови людини, а вторинними — перетворювачі різного типу, у тому числі электроакустичні. Останні являють собою пристрої, призначені для перетворення акустичних коливань в електричні й назад. До них відносяться пьезоэлементы, мікрофони, телефони, гучномовці й інші пристрої. Залежно від форми акустичних коливань розрізняють прості (тональні) і складні сигнали. *Тональний сигнал* — це сигнал, викликаний коливанням, що відбувається 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.

1.3. Середовища поширення акустичних каналів витоку інформації

Під технічним каналом витоку акустичної (мовленнєвої) інформації розуміють сукупність об'єкта розвідки (виділеного приміщення), технічного засобу акустичної (мовленнєвої) розвідки, за допомогою якого перехоплюється мовна інформація, та фізичного середовища, в якому поширюється інформаційний сигнал. Залежно від фізичної природи виникнення інформаційних сигналів, середовища їх поширення технічні канали витоку акустичної (мовленнєвої) інформації можна розділити на: прямі акустичні (повітряні), акустовібраційні (вібраційні), акустооптичні (лазерні), акустоелектричні та акустоелектромагнітні.

Повітряні канали. У повітряних технічних каналах витоку інформації середовищем поширення акустичних сигналів є повітря і у разі перехоплення інформації через повітряний канал витоку можливий запис мовної інформації портативними засобами запису, які потайно встановлені у приміщеннях. Так само можлива прихована установка пристроїв з датчиками мікрофонного типу; прослуховування і запис розмов за допомогою спрямованих мікрофонів.

Спрямовані мікрофони можуть бути встановлені в найближчих будовах або транспортних засобах. Мікрофони поєднуються або з'єднуються з портативними звукозаписними пристроями (диктофонами) або спеціальними мініатюрними передавачами.

Перехоплена інформація може передаватися по радіоканалу, оптичному каналу (в інфрачервоному діапазоні довжин хвиль), по мережі змінного струму, сполучним лініям, стороннім провідникам (трубам водопостачання й каналізації, металоконструкціям і т.п.). Причому для передачі інформації із труб і металоконструкцій можуть застосовуватися не тільки електромагнітні, але й механічні коливання.

Вібраційні канали. У вібраційних(структурних) каналах витоку інформації середовищем поширення акустичних сигналів є конструкції будинків При перехопленні інформації по вібраційному каналу витіку можливе приховане прослуховування і запис розмови з приміщень з використанням електронних стетоскопів. Також можлива прихована установка заставних пристроїв з датчиками контактного типу, які передають інформацію по радіо чи оптичним каналам.

Електроакустичні канали. Електроакустичні технічні канали витоку інформації виникають за рахунок електроакустичних перетворень акустичних сигналів в електричні. При перехопленні інформації по електроакустичному каналу витіку можливого підключення спеціальних низькочастотних підсилювачей до сполучних ліній ВТСС, що мають мікрофонний ефект, а також підключення апаратури високочастотного нав'язування до сполучних ліній ВТСС, що мають мікрофонний ефект.

Оптико-електронний канал. Оптико-електронний (лазерний) канал витоку інформації утвориться при опроміненні лазерним променем вібруючих в акустичному полі тонких поверхонь, що відзеркалюють (стекол, вікон, картин, дзеркал і т.д.). Відбите лазерне випромінювання (дифузійне або дзеркальне) модулюється по амплітуді й фазі (за законом вібрації поверхні) і приймається приймачем оптичного випромінювання, при демодуляції якого виділяється мовна інформація.

Параметричні канали**.** У результаті впливу акустичного поля міняється тиск на всі елементи високочастотних генераторів. При цьому змінюється взаємне розташування елементів схем, проводів у котушках індуктивності, дроселів і т.п., що може привести до змін параметрів високочастотного сигналу, наприклад, до модуляції його інформаційним сигналом. Тому цей канал витоку інформації називається параметричним. Це обумовлено тим, що незначна зміна взаємного розташування проводів у котушках індуктивності (межвиткового відстані) приводить до зміни їхньої індуктивності, а, отже, до зміни частоти випромінювання генератора, тобто до частотної модуляції сигналу. Точно так само вплив акустичного поля на конденсатори приводить до зміни відстані між пластинами й, отже, до зміни його ємності, що, у свою чергу, також приводить до частотної модуляції високочастотного сигналу генерації.

У електромагнітних каналах просочування інформації носієм інформації є електромагнітне випромінювання (ЕМІ), що виникає при обробці інформації технічними засобами :

- бічне електромагнітне випромінювання, що виникає при протіканні інформаційних сигналів через елементи технічних засобів обробки інформації;
- модуляція інформативним сигналом побічного електромагнітного випромінювання високочастотного генератора технічних засобів обробки інформації (на частотах ВЧ генератора);

– модуляція інформаційним сигналом паразитного електромагнітного випромінювання технічних засобів обробки інформації (наприклад, що виникають при самозбудженні підсилювачів низької частоти).

Під матеріальним каналом витоку можна розуміти безліч об'єктів в різних станах. Це можуть бути відходи виробництва, сировина або бракована продукція. Залежно від характеру і міри ушкодження його можна розділити на:

– фінансовий збиток, пов'язаний з витратами на відновлення інформаційної системи компанії, також із-за простоїв, викликаних змінами в системі захисту інформації;
– матеріальний і моральний збиток, заподіяний власникам інформації, чия інформація була викрадена і в результаті був нанесений збиток ділової репутації і діловим стосункам.

1.4. Технічні засоби отримання акустичної інформації

Перехоплення акустичної інформації за допомогою радіопередаючих засобів. До них ставиться широка номенклатура радіозакладок (радіомикрофонів, “жучків”), призначенням яких є передача по радіоканалу акустичної інформації, одержуваної на об'єкті.Застосування радіопередаючих засобів припускає обов'язкова наявність приймача, за допомогою якого здійснюється прийом інформації від радіозакладки. Приймачі використовуються різні - від побутових до спеціальних. Іноді застосовуються так називані автоматичні станції. Вони призначені для автоматичного запису інформації у випадку її появи на об'єкті.

Перехоплення акустичної інформації за допомогою ІЧ передавачів

Передача інформації може здійснюється по ІЧ каналу. Акустичні закладки даного типу характеризуються крайньою складністю їхнього виявлення. Строк роботи цих виробів - кілька діб, але варто мати на увазі, що прослухати їхню передачу можна лише на спецприймачі й тільки в прямому візуальному контакті, тобто безпосередньо бачачи цю закладку. Тому розміщаються вони біля вікон,

вентиляційних отворів і т.п., що полегшує завдання їхнього пошуку. Основне достоїнство цих закладок - скритність їхньої роботи.

Закладки, що використовують канали передачі акустичної інформації через мережу 220 V і телефонну лінію. Подібність цих закладок у тім, що вони використовують у своїй роботі принцип низькочастотного ущільнення каналу передачі інформації. Оскільки в “чистих” лініях (220 V) і телефонних лініях присутні тільки сигнали на частотах 50 Гц й 300–3500 Гц відповідно, то передавачі таких закладок, транслюючи свою інформацію на частотах 100–250 кГц, не заважають роботі цих мереж. Підключившись до цих ліній спецприемачем, можна знімати передану із закладки інформацію на дальності до 500 м

Диктофони

Диктофони - пристрої, що записують голосову інформацію на магнітний носій (стрічку, дріт, внутрішню мікросхему пам'яті). Час запису різних диктофонів коливається в межах від 15 хв. до 8 г..

Сучасні цифрові диктофони записують інформацію у внутрішню пам'ять, що дозволяє робити запис розмови тривалістю до декількох годин. Ці диктофони практично безшумні (тому що немає ні касети, ні механічного стрічкопротягувального механізму, що роблять основний шум), мають можливість скидання записаної інформації на пам'ять комп'ютера для її подальшої обробки (підвищення розбірливості мови, виділення корисних фонових сигналів і т.д.).

Провідні мікрофони

Провідні мікрофони встановлюються в приміщенні, що цікавить, і з'єднуються провідною лінією із прийомним пристроєм. Мікрофони встановлюються або потай (немасковані), або маскуються під предмети побуту, офісної техніки й т.д. Такі системи забезпечують передачу аудіосигналу на дальність до 20 м. При використанні активних мікрофонів - до 150 м. Кілька мікрофонів можуть заводитися на загальний комутуючий пристрій, що дозволяє одночасно контролювати кілька приміщень і здійснюючий запис перехоплених розмов на диктофон.

“Телефонне вухо”

Даний пристрій звичайно потай монтується або в телефоні, або в телефонній розетці. Працює він в такий спосіб. Людина, що хоче скористатися даним пристроєм (оператор), робить телефонний дзвінок на номер, на якому він “висить”. “Телефонне вухо” (ТВ) “проковтує” перші два дзвінки, тобто в контрольованому приміщенні телефонні дзвінки не лунають. Оператор кладе трубку й знову набирає цей номер. У трубці буде звучати сигнал “зайнято”, оператор чекає 30-60 с. (часовий пароль) і після припинення сигналу “зайнято” набирає бипером (генератором DTMF-посилок) задану кодову комбінацію (цифровий пароль). Після цього вмикається мікрофон ТВ й оператор чує все, що відбувається в контрольованому приміщенні практично з будь-якого місця в світі, де є телефонний апарат. Розрив зв'язку відбудеться, якщо оператор покладе трубку або якщо хтось підніме слухавку в контрольованому приміщенні. Для всіх інших абонентів, що бажають додзвонитися на цей номер, буде чутний сигнал “зайнято”. Даний алгоритм роботи є типовим, але може відрізнятися в деталях реалізації, залежно від вимог.

Апаратура, що використовує мікрофонний ефект телефонних апаратів

Прослуховування приміщень через телефон здійснюється за рахунок використання “мікрофонного ефекту”. Недолік методу полягає в тому, що “мікрофонним ефектом” володіють старі моделі телефонних апаратів, які зараз застосовуються рідко.

Апаратури ВЧ нав'язування

ВЧ коливання проходять через мікрофон або деталі телефону, що володіють “мікрофонним ефектом” і модулюються в акустичний сигнал із приміщення, де встановлений телефонний апарат. Промодульований сигнал демодулюється амплітудним детектором і після посилення подається на пристрій, що реєструє сигнал.

Як мікрофон може працювати й будинок. Спрямоване на нього випромінювання відповідної частоти модулюється (змінюється) спеціальними конструктивними елементами, які здатні вловлювати звукові коливання, що

виникають при розмові. Таким чином, відбите від будинку випромінювання в зміненому виді несе із собою інформацію про те, що було вимовлено усередині. Які фізичні процеси, явища, властивості матеріалів могли б сприяти реалізації такого способу знімання мовної інформації?

Розглянемо приклад резонансу звичайної слухавки. Тому що мікрофон має значно менше опір у порівнянні з телефонним капсулем, тоді (для простоти виложеного матеріалу) представимо еквівалентну схему у вигляді короткозамкненої лінії із проводами довжиною L і підсумовуючою паразитною ємністю С (Рис. 1.6).

Із графіків, представлених на рис. 1.7, видно, що струм на мікрофоні максимальний тоді, коли напруга прагне до нуля. Струм протікає через мікрофон і модулюється за законом низької частоти, а оскільки лінія в трубці далеко не ідеальна, то основна частина енергії з лінії перетворюється в електромагнітні коливання й випромінюється в ефір.

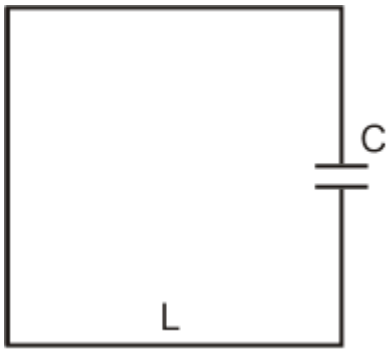

Рис. 1.6. Еквівалентна схема слухавки

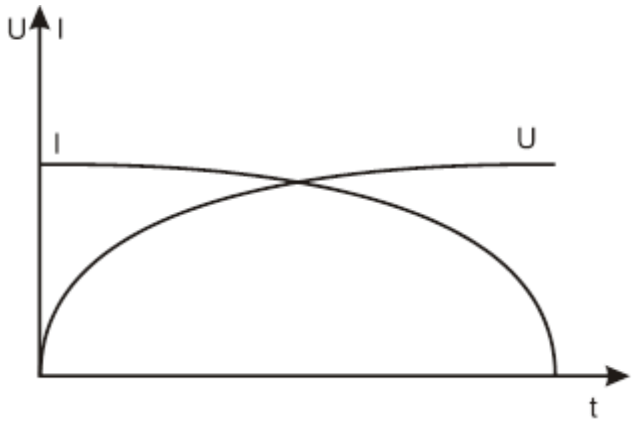

Рис. 1.7. Взаємна залежність струму й напруги на мікрофоні

Виходячи із правила наведених ЕРС, можна зробити вивід про те, що найбільша потужність наведеного сигналу досягається у випадку паралельного розташування слухавки й передавальної антени. При розташуванні їх під кутом відносно один одного ЕРС зменшується.

Як уже було показано раніше, наведений сигнал моделюється по амплітуді й випромінюється в ефір на тій же резонансній частоті, але оскільки цей сигнал значно слабкіше опромінює ВЧ сигнал на резонансній частоті, то й коефіцієнт модуляції стосовно частоти модуляції стає дуже малим.

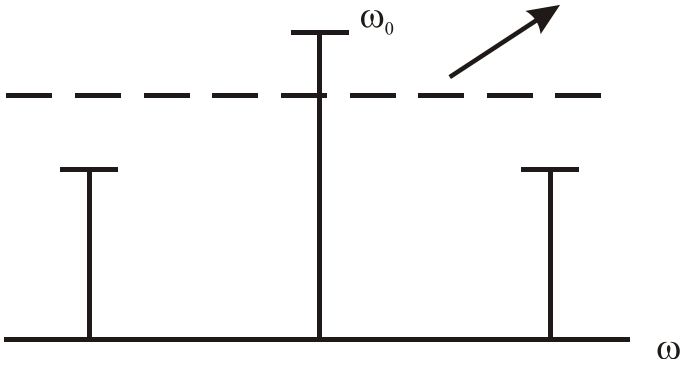

Рис. 1.8. Випромінювання модульованого сигналу

Для нормального прийому необхідно “обрізати” несучу так, щоб коефіцієнт модуляції став близько 30%. При потужності генератора на частоті 370 мГц рівної 40 мКвт вдалося домогтися впевненого прийому на дальності близько 100 м.

Виявилося, що на дальність прийому дуже сильно впливає відстань телефонного апарата від землі. Чим ближче він розташований до землі, тим більше поглинання електромагнітного поля (рис. 1.8). У розглянутому прикладі процес модуляції відбувається за рахунок зміни опору мікрофона телефонного апарата.

При опроміненні проводів, ліній зв'язку й т.п., що несуть аналогову або цифрову інформацію при $\omega_0 = \Delta/4$, модуляція що опромінює ВЧ сигналом відбувається легше, ніж у випадку з мікрофоном телефонного апарата.

Таким чином, знімання мовної інформації при опроміненні персонального комп'ютера або інших ланцюгів на великій відстані стає реальністю.

Розглянемо ланцюг, що несе інформацію у вигляді відеоімпульсів із широтною модуляцією (рис. 1.9).

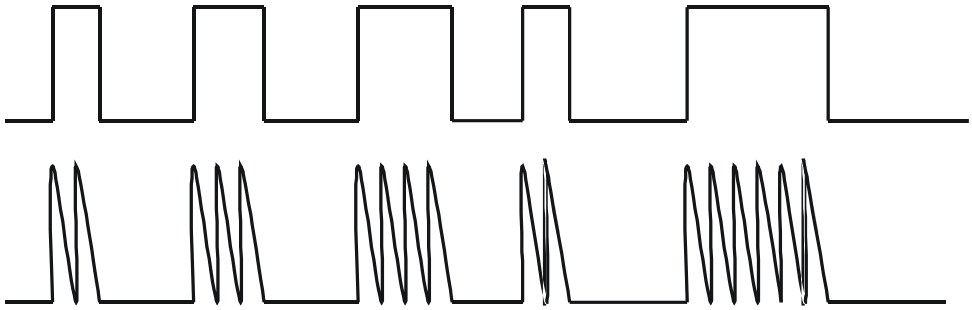

Рис. 1.9. Відеоімпульси із широтною модуляцією

Припустимо, що знайдено ділянку ланцюга з різкими вигинами проводів, по якому проходить інформація. Знаючи довжину цієї ділянки, можна визначити й резонансну частоту ω_0. При резонансі даної ділянки ланцюга відеоімпульси перетворяться в радіоімпульси й можуть перевипромінюватися на більші відстані, причому коефіцієнт модуляції в цьому випадку значно вище, ніж у випадку вже з відомою слухавкою.

Трохи інша схема застосування обговорюваного резонансного методу знімання мовної інформації з резонансних схем, у яких застосовуються картини в металізованих або металевих рамках.

Металева окантовка рами звичайно має розрив, а саме полотно містить у своєму составі (у фарбах) солі різних металів. Рамка, таким чином, — це один виток проведення **L**, а картина з підкладкою й оправою — ємність **C.** Причому при впливі мови полотно коливається, і **C** змінюється, тобто відіграє роль мембрани. Виходить **LC**-контур зі своєю резонансною частотою. Амплітудно-частотна характеристика уточнення **Q** показана на рис. 1.10.

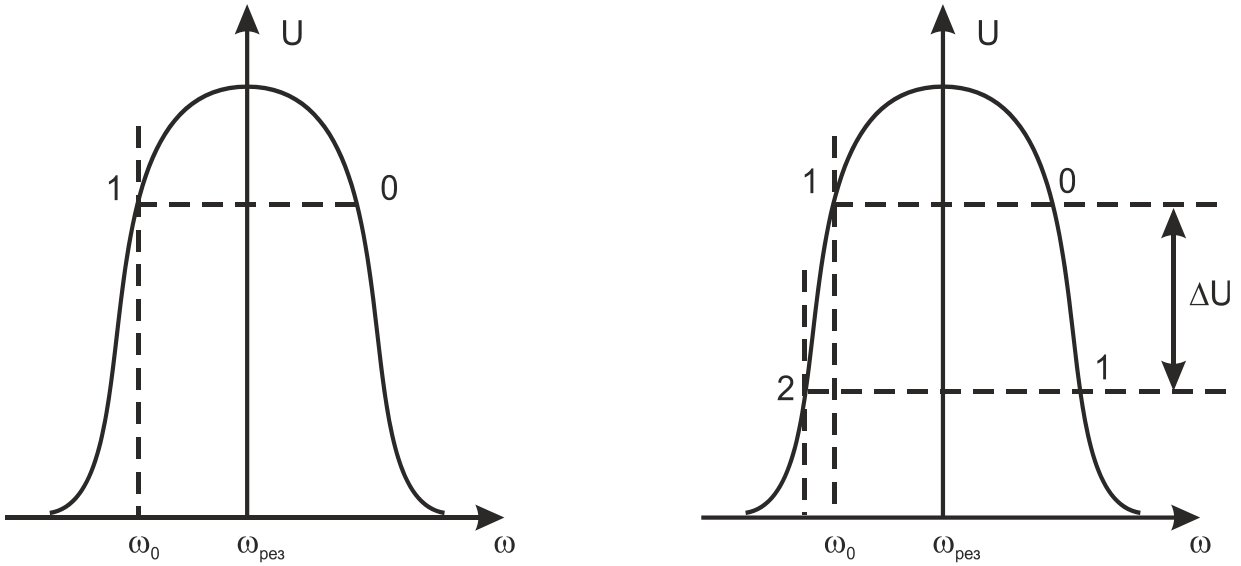

Рис. 1.10. Амплітудно-частотна характеристика при використанні резонансної схеми

Якщо дану систему опромінити не на частоті резонансу **ωрез**, а на схилі характеристики, то при зміні частоти **ωрез** (за рахунок зміни **C** під впливом звукових хвиль) при **ω0 = const** характеристика зрушується в ту або іншу сторону, і з'явиться **ΔU**, тобто амплітудна модуляція.

Цей канал витоку мовної інформації становить небезпеку ще й з погляду складності його виявлення службою безпеки об'єкта. Оскільки рівні випромінювань дуже малі, зафіксувати їх без складання радіомапи практично неможливо. Прийняти сигнал без спеціального прийомного пристрою також не представляється можливим. Всі існуючі системи захисту при даному методі знімання неефективні. Наприклад, шунтування мікрофона ємністю тільки

поліпшує визначення резонансної характеристики, тому що в крапці пучності струму напруга дорівнює нулю, і конденсатор не працює.

Стетоскопи - це пристрої, що перетворюють пружні механічні коливання твердих фізичних середовищ в акустичний сигнал. У сучасних стетоскопах таким перетворювачем слугує пьезодатчик. Данна апаратура в основному застосовується для прослуховування сусідніх приміщень через стіни, стелі, підлогу або через труби центрального опалення. Професійна апаратура цього класу компактна (міститься в кейсі середніх розмірів), автономна, має можливість підстроювання параметрів під конкретну робочу обстановку, здійснює запис отриманої інформації на диктофон. Стетоскопічні датчики часто доустатковуються радіопередавачем, що дозволяє прослуховувати перехоплену інформацію на скануєчому приймачеві, як від звичайної радіозакладки.

Лазерні стетоскопи

Лазерні стетоскопи - це пристрої, що дозволяють зчитувати лазерним променем вібрацію із предметів, промодульованих акустичним сигналом. Зазвичай, акустична інформація знімається із шибок. Сучасні лазерні стетоскопи добре працюють на дальності до 300 м. Недоліками цих апаратур є висока вартість (до 30 тис. доларів), необхідність просторового розносу джерела й приймача лазерного випромінювання, сильна залежність якості роботи від зовнішніх умов (метеоумови, сонячні відблиски й т.д.).

Спрямовані акустичні мікрофони (САМ)

Дана техніка призначена для прослуховування акустичної інформації з певного напрямку й з більших відстаней. Залежно від конструкції САМ, ширина головного променя діаграми спрямованості перебуває в межах 5–30°. По типу використовуваних антенних систем САМ бувають:

Дзеркальні (мікрофон САМ перебуває у фокусі параболічної антени). Відстань 500 м і більше, діаметр дзеркала становить до 1 м, діаграма спрямованості - до 8).

Мікрофон-трубка (звичайно маскується під тростину або парасоль), при цьому дальність дії до 300 м, а діаграма спрямованості - до 18 (При підвищенні рівня шумів до 60 дб дальність знижується до 100 м.).

САМ органного типу (більші мобільні або стаціонарні установки, зокрема, застосовувані в прикордонних військах для прослуховування акустичних сигналів із суміжної території й ін.), дозволяє здійснювати прослуховування до 1000 м. Плоскі САМ, що використають у якості антенної системи фазированих антенних ґрат (ФАГ), звичайно маскуються під кейс, у кришку якого монтується ФАГ. Акустична розвідка методом пасивного перехоплення заснована на перехопленні акустичної хвилі спрямованими мікрофонами.

Акустичні методи перехоплення - опромінення коливних предметів в УФ й ІЧ діапазонах, оптичним лазерним стетоскопом. Використовується також опромінення радіопроменем, але при цьому стійкий прийом інформації можливий на відстані 300-400 м. Ультразвукове знімання інформації можливе у всіх напрямках через широку діаграму спрямованості антеною системи й на відстані 300 м.

Контактні методи перехоплення (заставні пристрої):

- радіомікрофони безперервної дії;
- радіомікрофони з вимиканням живлення;
- радіомікрофони з керуванням по радіо;
- радіомікрофони з дистанційним живленням;
- стетоскопи.

Здійснюється знімання мовної інформації з наступних ланцюгів:

- дзвінковий ланцюг;
- реле;
- знімання інформації з вимірювальної головки вольтметрів й амперметрів;
- система радіотрансляції;
- система електрочасифікації;
- система пожежної й охоронної сигналізації.

1.5. Фізичні перетворювачі

У будь-яких технічних засобах існують ті або інші фізичні перетворювачі, що виконують відповідні їм функції, які засновані на певному фізичному принципі дії. Гарне знання всіх типів перетворювачів дозволяє вирішувати завдання визначення наявності можливих неконтрольованих проявів фізичних полів, що утворять канали витоку інформації.

Характеристики фізичних перетворювачів

Перетворювачем є прилад, що трансформує зміну однієї фізичної величини в зміну іншої. У термінах електроніки перетворювач звичайно визначається як прилад, що перетворює неелектричну величину в електричний сигнал або навпаки (рис. 1.11).

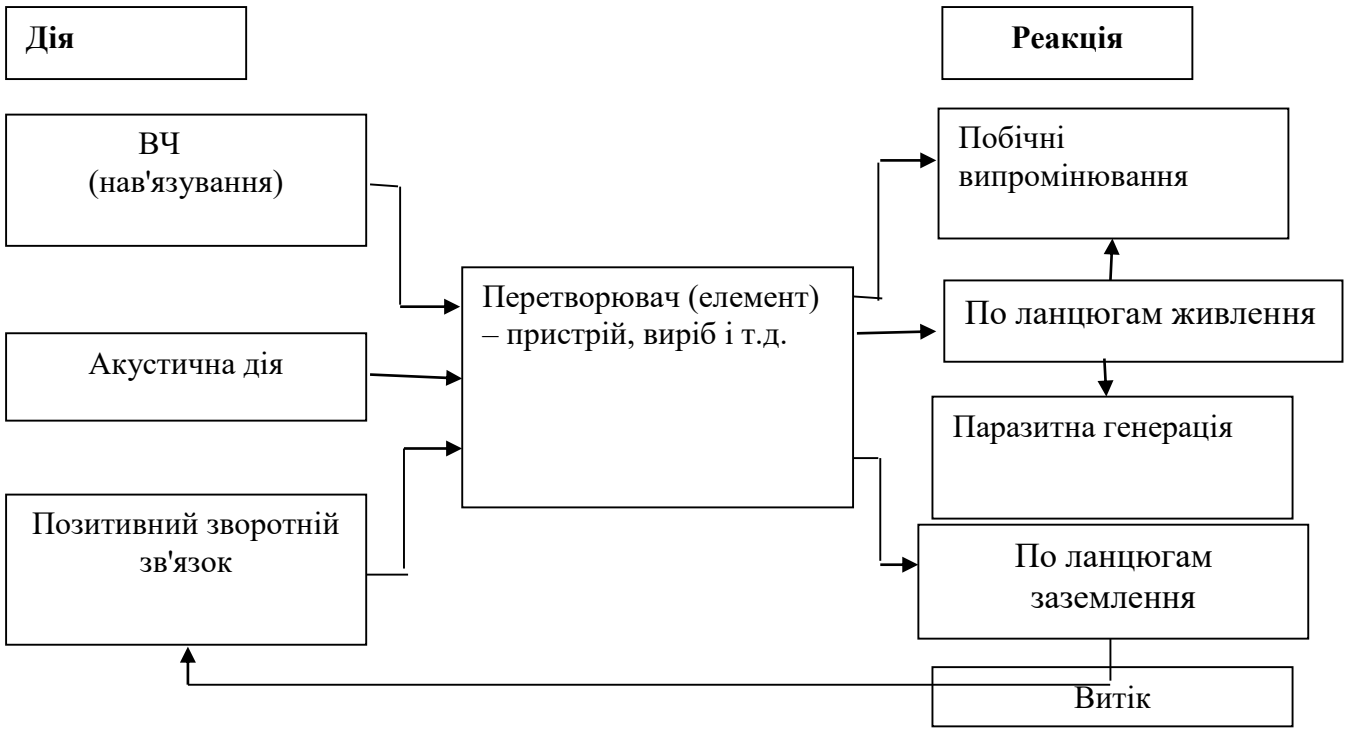

Рис. 1.11. Схема роботи перетворювача

Кожен перетворювач діє по певних фізичних принципах й утворює властивим цим принципам передавальний канал - тобто канал витоку інформації.

Функції приладів й електронних пристроїв можна розділити на два основних види - обробка електричних сигналів і перетворення якого-небудь зовнішнього фізичного впливу в електричні сигнали. У другому випадку основну роль виконують датчики й перетворювачі.

Різноманітні ефекти зовнішнього світу не обмежуються у своїх проявах лише електричними сигналами. Численні різні фізичні явища (звук, світло, тиск і т.д.) - їх можна нарахувати не менш декількох десятків. Для перетворення інформації про фізичні явища у форму електричного сигналу в електронних системах використаються чутливі елементи - датчики. Датчики є початком будь-якої електронної системи, граючи в ній роль джерел електричного сигналу.

Існують два види датчиків:

спеціально розроблені для створення необхідного електричного сигналу;

випадкові, що є результатом недосконалості схеми або пристрою.

За формою перетворення датчики можуть бути розділені на *перетворювачі сигналу* й *перетворювачі енергії*.

На перетворювач впливають певні сили, що породжують певну реакцію.

Будь-який перетворювач характеризується певними параметрами. Найбільш важливими з них є:

Чутливість. Це відношення зміни величини вихідного сигналу до зміни сигналу на його вході.

Розв'язна здатність, що характеризує найбільшу точність, з якої здійснюється перетворення.

Лінійність. Характеризує рівномірність зміни вихідного сигналу залежно від зміни вхідного.

Інертність, або час відгуку, що дорівнює часу встановлення вихідного сигналу у відповідь на зміну вхідного сигналу.

Смуга частот. Ця характеристика показує, на яких частотах впливу на вході ще сприймаються перетворювачем, створюючи на виході ще припустимий рівень сигналу.

По фізичній природі перетворювачі діляться на численні групи, серед яких слід зазначити фотоелектричні, термоелектричні, п'єзоелектричні, електромагнітні й акустоелектричні перетворювачі, що широко використаються в сучасних системах зв'язку, керування й обробки інформації (рис. 1.12).

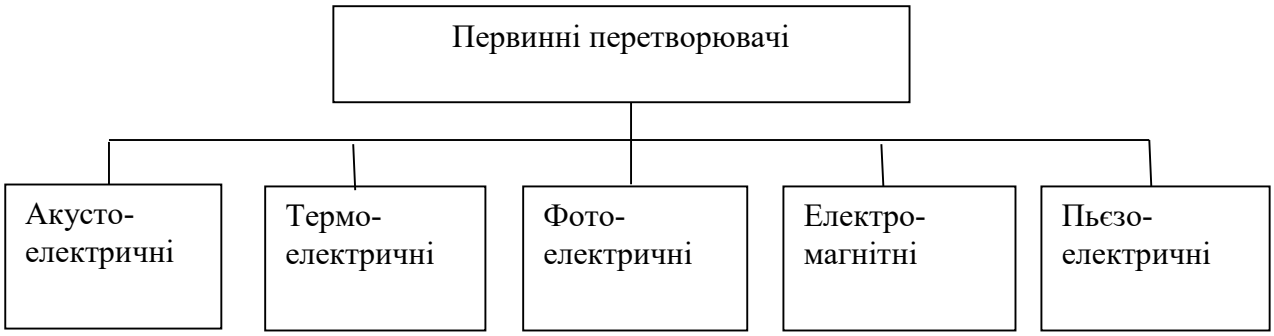

Рис. 1.12. Групи первинних перетворювачів

Види акустоелектричних перетворювачів

Акустична енергія, що виникає під час звучання мови, може викликати механічні коливання елементів електронних апаратур, що у свою чергу приводить до появи електромагнітного випромінювання або його зміні при певних обставинах. Види акустоэлектрических перетворювачів представлені на Рис. 1.13. Найбільш чутливими до акустичних впливів елементами радіоелектронних апаратур є котушки індуктивності й конденсатори змінної ємності.

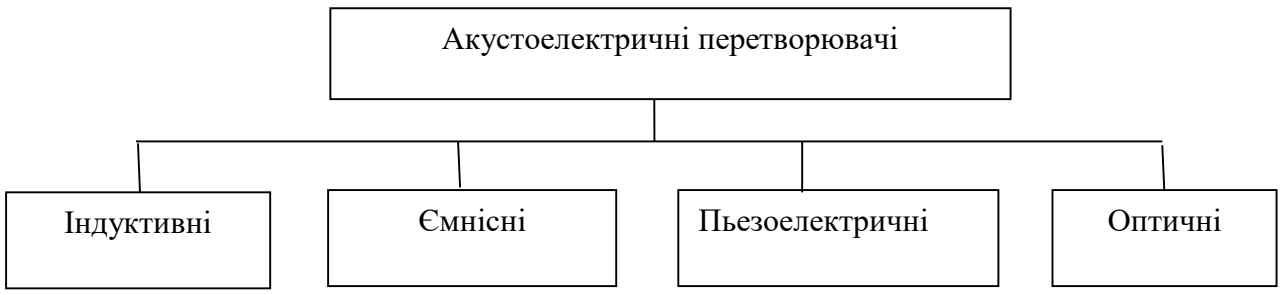

Рис. 1.13. Види акустоелектричних перетворювачів

Індуктивні перетворювачі

Якщо в поле постійного магніту помістити котушку індуктивності (рамку) і привести її в обертання за допомогою, наприклад, повітряного потоку (рис. 1.14), то на її виході з'явиться ЕРС індукції.

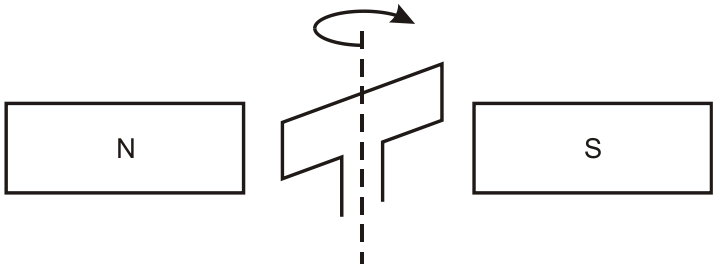

Рис. 1.14. Обертання рамки в магнітному полі приводить до генерації ЕРС

Під час звучання людської мови виникає повітряний потік змінної щільності. Раз так, то очікується, що під впливом повітряного потоку мови буде обертатися й котушка (рамка), що викличе пропорційну зміну ЕРС індукції на її кінцях. Так можна зв'язати акустичний вплив на провідник у магнітному полі з виникаючої ЕРС індукції на його кінцях. Це типовий приклад групи індукційних акустичних перетворювачів. Представником цієї групи є, наприклад, електродинамічний перетворювач.

Розглянемо акустичний вплив на котушку індуктивності із сердечником (рис. 1.15). Механізм й умови виникнення ЕРС індукції в такій котушці зводяться до наступного:

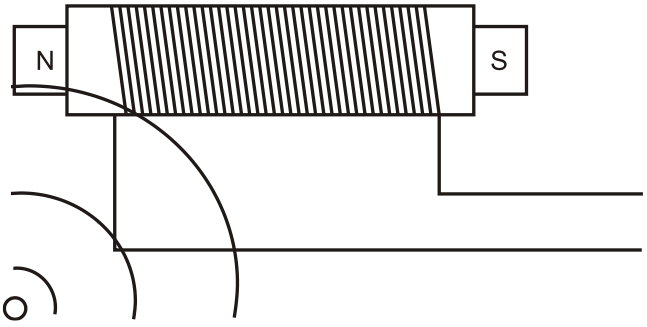

Рис. 1.15. Виникнення ЕРС на котушці індуктивності

Під акустичним тиском Р з'являється вібрація корпуса й обмотки котушки. Вібрація викликає коливання проводів обмотки в магнітному полі, що й приводить до появи ЕРС індукції на кінцях котушки. Виникнення ЕРС на вході такого перетворювача прийнято називати мікрофонним ефектом. Можна затверджувати, що мікрофонний ефект здатний проявлятися як в електродинамічної, так й в електромагнітній, конденсаторній й іншій конструкціях, широко використовуваних у мікрофонах всілякого призначення й використання.

Мікрофонний ефект електромеханічного дзвінка телефонного апарата

Електромеханічний викличний дзвінок телефонного апарата - типовий зразок індуктивного акустоелектричного перетворювача, мікрофонний ефект якого проявляється при покладеній мікротелефонній трубці.

ЕРС мікрофонного ефекту дзвінка (рис. 1.16) може бути визначена по формулі:

$$E_{МЭ} = \eta P,$$

де η— акустична чутливість дзвінка, **P** — акустичний тиск, $\eta = \frac{VS\mu_0 NS_M}{d^2 Z_M}$;

де **V** — магніторушійна сила постійного магніту; **S** — площа якоря (пластини); μ_0 — магнітна проникність сердечника; **N** — кількість витків котушки; S_M — площа полосного наконечника; **d** — величина зазору; Z_M — механічний опір.

По такому ж принципу (принципу електромеханічного викличного дзвінка) утвориться мікрофонний ефект й в окремих типах електромеханічних реле різного призначення й навіть в електричних викличних дзвінках побутового призначення. Акустичні коливання впливають на якір реле (рис. 1.18). Коливання якоря змінюють магнітний потік реле, що замикається по повітрю і приводить до появи на виході котушки реле ЕРС мікрофонного ефекту.

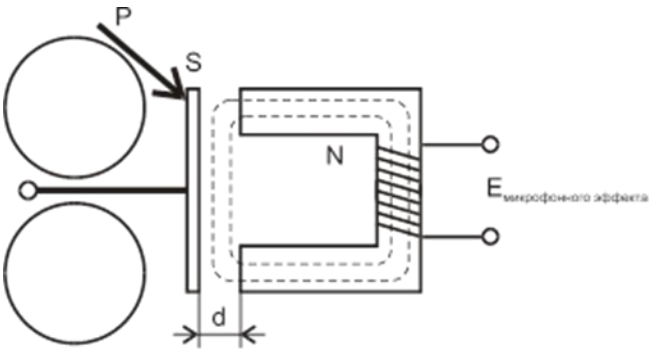

Рис. 1.16. Схема виникнення ЕРС на викличному дзвінку

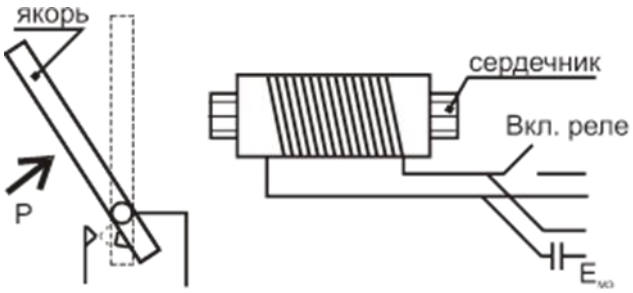

Рис. 1.17. Схема виникнення ЕРС на реле

Динамічні головки прямого випромінювання, установлювані в абонентських гучномовцях, мають досить високу чутливість до акустичного впливу (2-3 мв/Па) і порівняно рівномірну в мовному діапазоні частот амплітудно-частотну характеристику, що забезпечує високу розбірливість мовних сигналів.

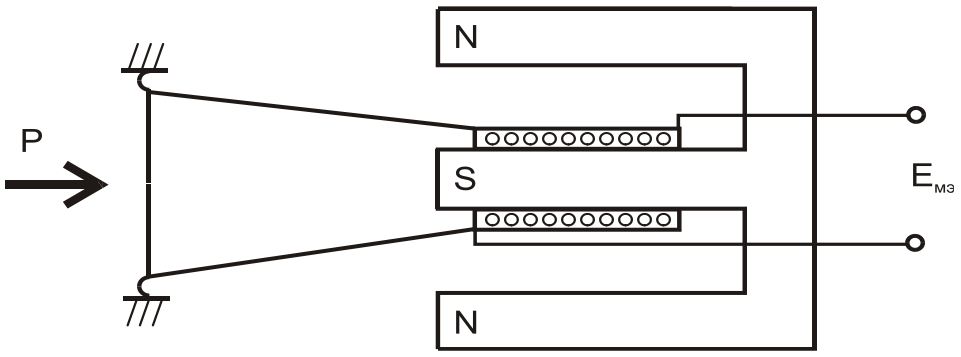

Рис. 1.17. Схема виникнення ЕРС на гучномовці

Відомо, що абонентські гучномовці бувають одне- і багатопрограмними. Зокрема, території колишнього СРСР досить широко поширені трьохпрограмні

гучномовці. Трьохпрограмні абонентські гучномовці, відповідно до ДЕРЖСТАНДАРТ 18286-88 (“Приймачі трьохпрограмні провідного віщання. Загальні технічні умови”), мають основний канал (НЧ) і канали радіочастоти (ВЧ), включені через підсилювач-перетворювач. Підсилювач-перетворювач забезпечує перетворення ВЧ сигналу в НЧ сигнал зі смугою (100-6300 Гц за рахунок використання убудованих гетеродинів. Так, наприклад, у трехпрограммном гучномовці “Маяк 202” використається два гетеродини для другої й третьої програм ВЧ. Один виробляє частоту 78 кгц, а іншої - 120 кгц.

Наявність складної електронної схеми побудови трехпрограммных гучномовців (зворотні зв'язки, взаємні переходи, гетеродини) сприяє прямому проникненню сигналу, наведеного в динамічній головці, на вхід пристрою (у лінію). Не виключається й випромінювання наведеного сигналу на частотах гетеродина (78 й 120 кгц).

Мікрофонний ефект вторинного електрогодинника

Виконавчий пристрій вторинного електрогодинника являє собою кроковий електродвигун, керований трьохсекундними різнополярними імпульсами **U** = ± 24 V, що надходять із інтервалом 57 від первинного єлектрогодинника.

Мікрофонний ефект вторинних годин, обумовлений акустичним ефектом крокового електродвигуна (рис. 1.19), проявляється в основному в інтервалах очікування імпульсів керування.

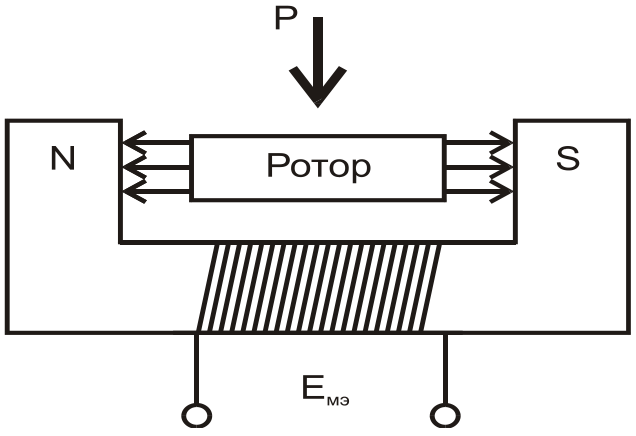

Рис. 1.19. Схема виникнення ЕРС на кроковому двигуні

Ступінь прояву мікрофонного ефекту вторинного електрогодинника істотно залежить від його конструкції, тобто чи виконані вони в пластмасовому, дерев'яному або металевому корпусі; з відкритим або закритим механізмом; із твердим або підвісним кріпленням.

Висновки по розділу. Проведено аналіз існуючих каналів витоку інформації. Встановлені причини виникнення акустичних каналів витоку інформації. Детально розглянуто фізичне підгрунття виникнення акустичних каналів витоку інформації.

2 ДОСЛІДЖЕННЯ ЗАСОБІВ ЗАХИСТУ ВІД ВИТОКУ ІНФОРМАЦІЇ ПО АКУСТИЧНОМУ КАНАЛУ

2.1. Технічні засоби несанкціонованого доступу

Розглянемо декілька найбільш поширені засоби знімання інформації по акустичному каналу:

- Електронні і лазерні стетоскопи
- Направлені мікрофони
- Радіозакладки

2.1.1. Електронні і лазерні стетоскопи

Електронні стетоскопи застосовують для зняття акустичної інформації через стіни, стелю, підлогу, труби опалення, вікна контрольованого приміщення. Оснований на принципу підсилання звуку, шумів.

У тому випадку, якщо не вдається проникнути навіть на короткий час в контрольоване приміщення, але є можливість доступу в сусідні приміщення, для ведення розвідки використовуються електронні стетоскопи, які перетворять акустичні коливання в твердих тілах (стінах, стелях, полі і так далі) в електричні.

Датчики електронних стетоскопів можуть бути встановлені в стінах будівель на етапах будівництва або реконструкції. В основному для передачі інформації використовується радіоканал, тому такі пристрої часто називають радіостетоскопами.

У тому випадку, коли вимагається прослухати розмови в закритому приміщенні на значній відстані, використовуються ЛАСР. ЛАСР складається з джерела когерентного випромінювання (лазера) і приймача оптичного

випромінювання, оснащеного фокусуючою оптикою. Принцип дії системи полягає в наступному. Передавач здійснює опромінення зовнішньої шибки вузьким лазерним променем. Приймач приймає розсіяне відбите випромінювання, що модулюється по амплітуді і фазі за законом зміни акустичного (мовного) сигналу, що виникає при веденні розмов в контрольованому приміщенні. Прийнятий сигнал демодулюється, посилюється і прослуховується на головних телефонах або записується на магнітофон. В даному випадку віконне скло виступає в ролі мембрани великої площі, на яку діє енергія звукової хвилі і приводить її в рух. Промінь лазера досягає поверхні скла і відбивається. Фотоприймач, входить до складу приладу для зняття інформації, реєструє відбитий промінь і перетворює світлову енергію в електричний сигнал, підсилює цей сигнал і відтворює за допомогою гучномовця або навушника. Так як скло коливається під впливом звуку, лазерний промінь буде відображатися під різним кутом, відповідно фотоприймач буде реєструвати і перетворювати світлову енергію відбитого луча в електричні коливання з різною амплітудою. В кінцевому рахунку, гучномовець приладу відтворює звукову інформацію контрольованого приміщення. Звичайно, серійні вироби більш складні.

Однак на якість інформації, що приймається, крім параметрів системи впливають такі чинники:

– параметри атмосфери (розсіювання, поглинання, турбулентність, рівень фону);

– якість обробки зондіруемої поверхні (шорсткості і нерівності, зумовлені як технологічними причинами, так і впливом середовища - бруд, подряпини і ін.);

– рівень фонових акустичних шумів;

– рівень перехопленого мовного сигналу.

Крім того, застосування подібних засобів вимагає великих витрат не тільки на саму систему, а й на обладнання з обробки отриманої інформації. Застосування такої складної системи вимагає високої кваліфікації і серйозної підготовки

операторів. З усього цього можна зробити висновок, що застосування лазерного знімання мовної інформації дороге задоволення і досить складне.

2.1.2. Направлені мікрофони

Якщо потрібно організувати прослуховування розмов в приміщенні, доступ до якого так само, як і доступ в сусідні приміщення, неможливий, то використовуються спрямовані мікрофони та лазерні акустичні локаційні системи. Спрямовані мікрофони мають коефіцієнт посилення більш 70 ... 90 дБ і дозволяють прослуховувати розмови на відстані до 300 ... 500м (в умовах міста-до 50...70м). Основні характеристики спрямованих мікрофонів: вид мікрофона, дальність перехоплення, розміри частотний діапазон, коефіцієнт посилення, діаграма спрямованості

Існує, як найменш чотири види направлених мікрофонів:

1. Параболічні;
2. Трубчасті, чи мікрофони "хвилі, що біжить";
3. Плоскі акустичні фазовані решітки;
4. Градієнтні;

Параболічний мікрофон представляє собою віддзеркалювач звуку параболічної форми, у фокусі якого міститься звичайний (ненаправлений) мікрофон. Віддзеркалювач виробляється як з оптично непрозорого, так і прозорого (наприклад, акрилової пластмаси) матеріалу. На рис. 2.1 пояснюється принцип роботи параболічного мікрофона. Величина зовнішнього діаметру параболічного дзеркала може бути від 200 до 500 мм. Звукові хвилі з усього напряму, віддзеркалюючись від параболічного дзеркала, сумуються у фазі в фокальній точці А. Виникає підсилення звукового поля. Чим більше діаметр дзеркала, тим більше підсилення може дати пристрій. Якщо напрям приходу звуку не вісьовий, то додавання віддзеркалених від різних частин параболічного дзеркала звукових хвиль, які приходять в точку А, дає менший результат, тому що не всі додатки

будуть в фазі. Послаблення тим сильніше, чим більше кут приходу звуку по відношенню до вісі. Утворюється, таким чином, кутова відбірковість за прийомом. Параболічний мікрофон є типовим прикладом високочутливого, але слабконаправленного мікрофону. Прикладом є направлений мікрофон "Велике вухо", що випустили в ФРН.

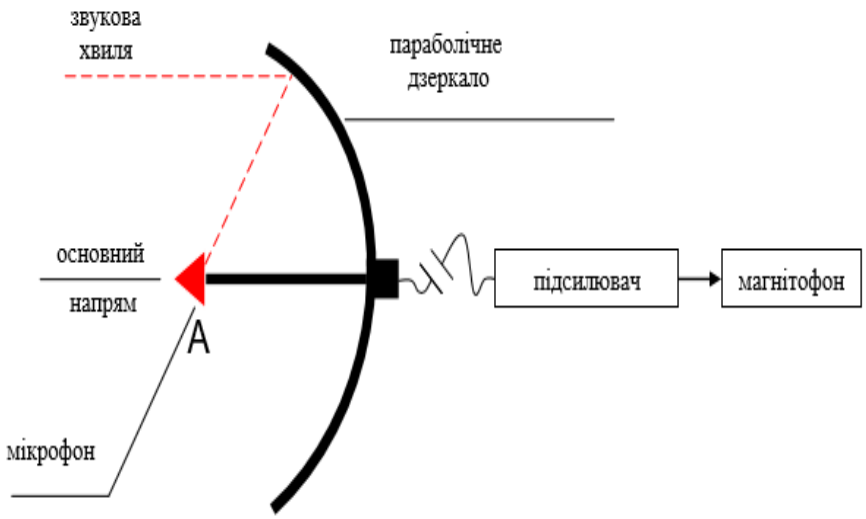

Рис.2.1. Параболічний мікрофон

Плоскі фазовані решітки реалізують ідею одночасного прийому звукового поля у дискретних точках деякої площини, перпендикулярної до напряму на джерело звуку (рис.2.2.). В цих точках (А1, А2, А3...) розміщуються чи мікрофони, вхідні сигнали яких сумуються електричними, чи, і частіше за все, відкриті торці звуководів, наприклад трубки достатньо малого діаметру, які забезпечують синфазне додавання звукових полів від джерела в деякому акустичному суматорі.

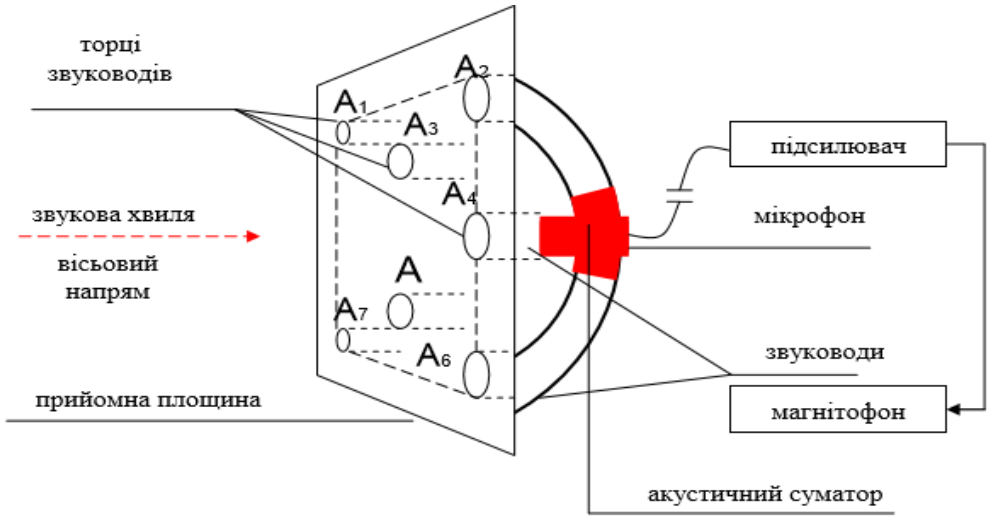

Рис.2.2. Плоска фазована рещітка

До виходу суматора підключений мікрофон. Якщо звук приходить з вісьового напряму, то всі сигнали, які розповсюджуються по звуководам, будуть у фазі, і додання в акустичному суматорі дасть максимальний результат. Якщо напрям на джерело звуку не вісьовий, а під деяким кутом до вісі, то сигнали від різних точок приймальної площини будуть різними за фазою та результат їх додання буде меншим. Чим більше кут приходу звуку, тим сильніше його послаблення. Звичайно число приймальних точок Ai у таких решітках складає декілька десятків. Конструктивно плоскі фазовані решітки вбудовуються або в передню стінку атташе-кейса з послідуючим камуфляжем, чи в майку-жилет, яка надягається під одежу (піджак чи сорочку). Необхідні електроні блоки (підсилювач, елементи живлення, магнітофон) розміщуються відповідно або в кейсі, або під одежею. Таким чином, плоскі фазовані решітки з камуфляжем візуально більш конспіративні у порівнянні з параболічним мікрофоном.

Так звані "плоскі" направлені мікрофони представляють собою акустичну антенну решітку, яка включає декілька десятків мікрофонів. Вони можуть вбудовуватися в стінку чи взагалі носитися у вигляді жилету під сорочкою чи піджаком. Дальність їхньої дії порівняно нижча за підношенням до перших двох типів направлених мікрофонів та сягає 30...50 м.

Трубчасті мікрофони, чи мікрофони "хвилі, що біжить", на відміну від параболічних мікрофонів та плоских акустичних решіток, приймають звук не на площині, а вздовж деякої лінії, співпадаючої з напрямом на джерело звуку.

Основою мікрофону є звукоприймач у вигляді жорсткої полої трубки діаметром 10-30 мм із спеціальними щілинними отворами, розміщеними рядами по всій довжині звуководу, з кутовою геометрією розміщення для кожного з рядів. При прийомі звуку з вісьового напряму буде відбуватися додавання в фазі сигналів, проникаючих в звуковід через усі щілинні отвори, так як швидкості вісьового розповсюдження звуку поза трубкою та всередині однакові. Коли ж звук приходить під деяким кутом до вісі мікрофону, це призводить до фазового неузгодження, так як швидкість звука в трубці буде більшою ніж вісьова складова швидкості звуку поза неї, внаслідок чого знижується чутливість прийому.

Звичайно довжина трубчастого мікрофону від 15-230 мм до 1 м. Чим більше його довжина, тим сильніше придушуються складові з бічного і тильного напрямів. Дальність прийому сигналів подібних мікрофонів може бути збільшена за рахунок використання більшого числа трубчастих елементів. "Мікрофон-труба" може бути закамуфльований під зонт чи трость або виконаний у звичайному вигляді. Характерним представником такого типу мікрофонів є мікрофон "Акустична рушниця".

Градієнтні мікрофони високих порядків на ринку відкритих пропозицій практично не представлені. Винятком є градієнтний мікрофон першого порядку. На відміну від фазованих приймальних акустичних решіток, які використовують операцію складання акустичних сигналів, градієнтні мікрофони основані на операції віднімання за напрямом приходу сигналу. Це ставить їх апріорі у невигідне положення по пороговій чутливості, тому що кожне віднімання послаблює сигнал, але статистично складає внутрішні вади.

В той же час сама по собі операція віднімання дозволяє конструювати направлені системи малих розмірів.

Він представляє собою два мініатюрних та близько розміщених високочутливих мікрофони, вихідні сигнали котрих електричні (чи акустичні)

віднімаються один від іншого, реалізуючи у кінцевих різницях першу похідну звукового поля віссю мікрофону та формуючи діаграму вигляду cos Q, де Q - кут приходу звуку. Тим самим забезпечується відносні послаблення акустичних полів з бічних напрямів (О - 90°). Градієнтними мікрофонами високих порядків називають системи, реалізуючи просторові похідні 2-го, З-го та більш високих порядків.

2.1.3. Радіозакладки

Радіозакладки працюють як звичайний передавач.В якості джерела електроживлення радіозакладок використовуються малогабаритні акумулятори. Термін роботи подібних закладок визначається часом роботи акумулятора. При безперервній роботі це 1-2 доби. Закладки можуть бути досить складними (використовувати системи накопичення і передачі сигналів, пристрої дистанційного накопичення).

Найпростіші радіозакладки включають три основних вузла, які визначають їх тактико-технічні можливості. Це: мікрофон, що визначає зону акустичної чутливості радіозакладки; власне радіопередавач, що визначає дальність її дії і скритність роботи; джерело електроживлення, визначальний час безперервної роботи.

Скритність роботи радіозакладок забезпечується невеликою потужністю передавача, вибором частоти випромінювання, обмеженням часу безперервної роботи (включати за допомогою дистанційного керування тільки коли це необхідно або короткочасна передача попередньо накопиченої інформації), а також застосуванням спеціальних заходів закриття. Часто робочу частоту вибирають поблизу несучої частоти потужної радіостанції, яка своїми сигналами маскує працюючу закладку.

Закриття радіоканалу застосовують різних видів: скремблирование (шифрування) переданого сигналу методом аналогового маскування сигналу у

вигляді інверсії низькочастотного спектра або адаптивної дельта-модуляції інформаційного сигналу з додаванням цифрового псевдовипадкового потоку. Радіомікрофони із закритим каналом важче виявляються навіть із застосуванням високовартісних пошукових технічних засобів, але і ціни на радіомікрофони із закритим каналом значно вище.

Використовувані в радиозакладке мікрофони можуть бути вбудованими або виносними. Фізична скритність радіозакладок визначається ретельної їх маскуванням в контрольованому приміщенні. Проте в кожному приміщенні є цілий ряд пристроїв, які виглядають цілком необразливо і можуть знаходиться на видному місці, не викликаючи навіть найменшої підозри, бо найчастіше радіомікрофони виготовляються в камуфльованому вигляді (авторучки, запальнички, картонки, предмети інтер'єру і т.д.) .

Дальність дії радіомікрофонів в основному залежить від потужності передавача, несучої частоти, виду модуляції і властивостей приймального пристрою.

Час безперервної роботи багато в чому залежить від організації живлення виробу. Якщо радіомікрофон живиться від мережі 220В, а такого типу "закладки" найчастіше виконуються у вигляді трійників, розеток, подовжувачів, то час роботи не обмежена. Якщо живлення здійснюється від батарей або акумуляторів, то вихід з положення знаходять у застосуванні режиму акустопуска (управління голосом), використання дистанційного керування (ДК) включенням або збільшенням ємності батарей.

З цього короткого опису випливає, що дальність дії, габарити і час безперервної роботи дуже взаємопов'язані. Справді, для збільшення дальності треба підняти потужність передавача, одночасно зростає струм споживання від джерела живлення, а значить скорочується час безперервної роботи. Щоб збільшити цей час, збільшують ємність батарей живлення, але при цьому ростуть габарити радіомікрофона. Крім того, слід враховувати, що збільшення потужності передавача знижує його скритність, тобто його легше виявити застосовуючи навіть не дуже складну і дорогу пошукову техніку.

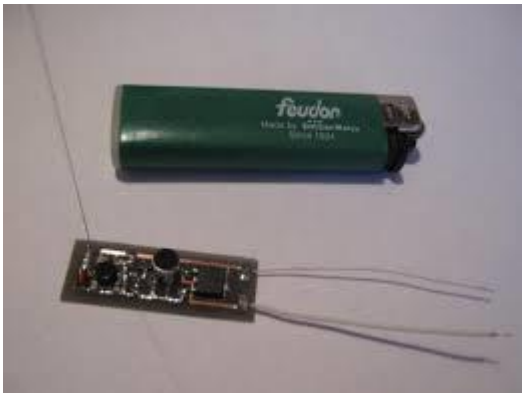

Рис.2.3. Радіозакладка

2.2. Технічні засоби захисту інформації по акустичному каналу

Засоби технічного захисту інформації - технічні засоби, основне функціональне призначення яких - захист інформації від загроз витоку, порушення цілісності та блокування; технічні засоби, у яких додатково до основного призначення передбачено функції захисту інформації; засоби, що призначені, спеціально розроблені або пристосовані для пошуку закладних пристроїв, які створюють загрозу для інформації, або контролю ефективності технічного захисту інформації.Основін з засобівзахисту по акустичному каналу є:

- Генератори шуму в акустичному діапазоні
- Пристрої віброакустичного захисту
- Технічні засоби ультразвукового захисту приміщень

2.2.1. Генератори шуму в акустичному діапазоні

Основний принцип радіоелектронної протидії – створення перешкод для приймального пристрою з інтенсивністю, достатньою для порушення його роботи.

Якщо наперед невідома його робоча частота, то необхідно створити перешкоду по всьому можливому або доступному діапазону спектру. Достатньо універсальною перешкодою для зв'язних радіоліній вважається шумовий сигнал, схема джерела шуму Рис.2.4. У зв'язку з цим апаратура радіопротидії повинна включати в свій склад генератор шуму достатньої потужності (на необхідний діапазон) і антенну систему. Практично при відношенні верхньої і нижньої частоти діапазону більш 2 х використовують декілька шумових генераторів і комбінована багатодіапазонна антена.

Рис.2.4. Структурна схема джерела акустичного шуму

Генератори шуму в мовному діапазоні використовуються для захисту від несанкціонованого знімання акустичної інформації шляхом маскування безпосередньо корисного звукового сигналу. Маскування проводиться "білим шумом" з коректованою спектральною характеристикою.

В деяких випадках наявність декількох випромінювачів необов'язково. Тоді використовуються компактні генератори з вбудованою акустичною системою, акустичний генератор білого шуму.

Головний недолік застосування джерел шумів в акустичному діапазоні – це неможливість комфортного проведення переговорів. Практика показує, що в приміщенні де "реве" генератор шуму неможливо знаходитися більше 10...15 мин. Крім того, співбесідники автоматично починають намагатися перекричати засіб захисту, знижуючи ефективність його застосування. Тому подібні системи

застосовуються для додаткового захисту дверних отворів, міжрамного простору вікон, систем вентиляції і т.д.

2.2.2. Пристрої віброакустичного захисту

Пристрої віброакустичного захисту використовуються для захисту приміщень, призначених для проведення конфіденційних заходів, від знімання інформації через шибки, стіни, системи вентиляції, труби опалювання, двері і т.д. Дана апаратура дозволяє запобігти можливому прослуховуванню за допомогою дротяних мікрофонів, звукозаписної апаратури, радіомікрофонів і електронних стетоскопів, лазерного знімання акустичної інформації з вікон і т.д. Протидія прослуховуванню забезпечується внесенням віброакустичних шумових коливань в елементи конструкції будівлі.

Елементами вібро-акустичних каналів витіку інформації, де джерелами конфіденційних даних виступають люди і технічні пристрої. Середовищем поширення виступають приміщення, що захищають конструкції трубо-проводы повітря. Засобами знімання можуть виступати різні пристрої наприклад стетоскоп лазерний мікрофон контактний мікрофон радіо, і дротяний мікрофон, і інші жучки для вібро-акустичного захисту будівель застосовують генератор білого або рожевого шуму і системи вібраційних зашумів, які укомплектовуються найчастіше такими пристроями як електромагнітні і пезоелектричні вібро-перетворювачі на основі пєзо-керамики. Для активного захисту повітряних каналів застосовують системи вібро-зашумлення до виходів яких підключають гучномовець який перевищує рівень сигналу у всьому частотному діапазоні (відношення сигнал / перешкода менш – 20 дБ).

2.2.3. Технічні засоби ультразвукового захисту приміщень

Найціннішою особливістю цих засобів є дія на мікрофонний пристрій, тому як його підсилювач робить потужний ультразвуковий сигнал (групу сигналів), що викликає блокування підсилювача або появу значних нелінійних спотворень, що призводять до порушення працездатності мікрофонного пристрою (його пригніченню).

Дія здійснюється по каналу сприйняття акустичного сигналу, тому його подальші трансформації і способи передання не важливі. Акустичний сигнал глушиться саме на етапі його сприйняття чутливим елементом. Усе це робить комплекс універсальним в порівнянні з іншими засобами захисту. А ще, при цьому апаратура майже не заважає роботі іншим пристроїм в кімнаті.

2.3. План приміщення і загрози

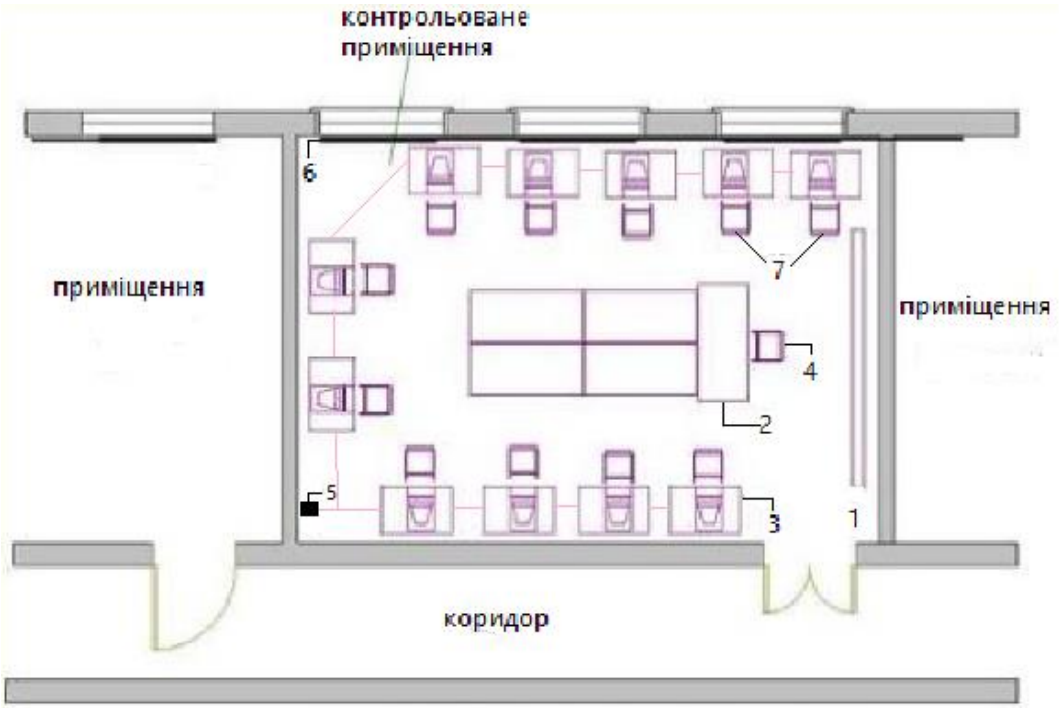

Рис.2.5. План приміщення

1- Дошка для написання

2 - Столи для засідання

3 - Робочі столи з комп’ютерами

4- Крісло керівника

5 - Система електроживлення, заземлення

6- Система опалення

7- Стільці для працівників

В даному приміщенні можливий витік акустичними каналами. 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. Подолавши огороджувальну конструкцію, частина енергії віброакустичних коливань (частина відбивається) перетворюється на акустичну і випромінюється у вигляді акустичних коливань.

Схематично шляхи витоку акустичної інформації за межі огороджувальних конструкцій відображені на рисунку 2.6.

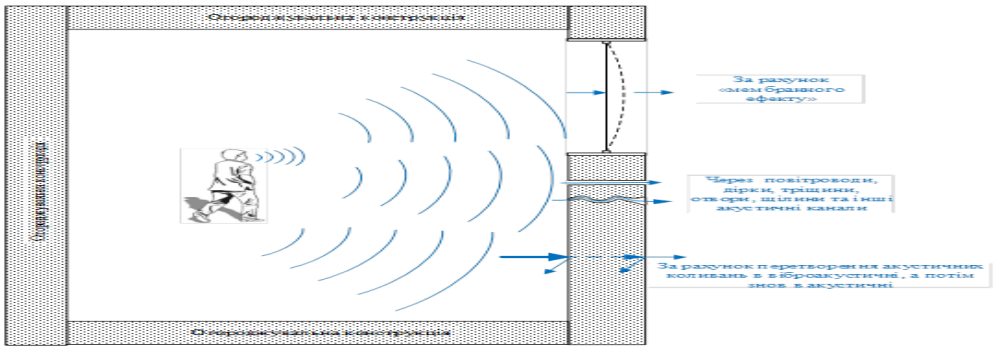

Рис. 2.6. Схема витоку акустичної інформації за межі конструкції

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.

Схематично канали витоку акустичної інформації відображені на рисунку.2.7.

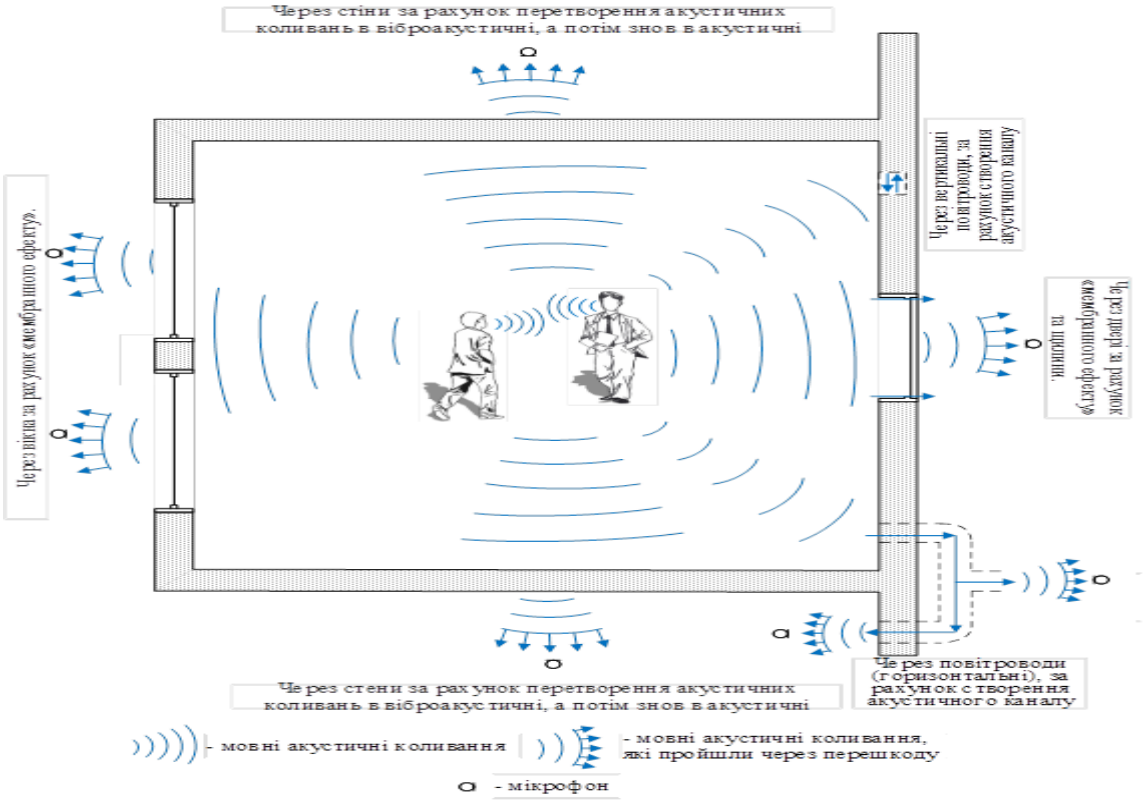

Рис.2.7. Канали витоку акустичної інформації

У віброакустичних каналах витоку інформації середовищем поширення мовних сигналів є огороджувальні будівельні конструкції приміщень (стіни, вікна, двері, перекриття тощо) та інженерні комунікації. Для перехоплення мовних сигналів у цьому випадку використовують контактні мікрофони (акселерометри).

Вібродатчик, з'єднаний з електронним підсилювачем називають електронним стетоскопом (далі - ЕС). ЕС дозволяє здійснювати прослуховування мови за допомогою головних телефонів та її запис.

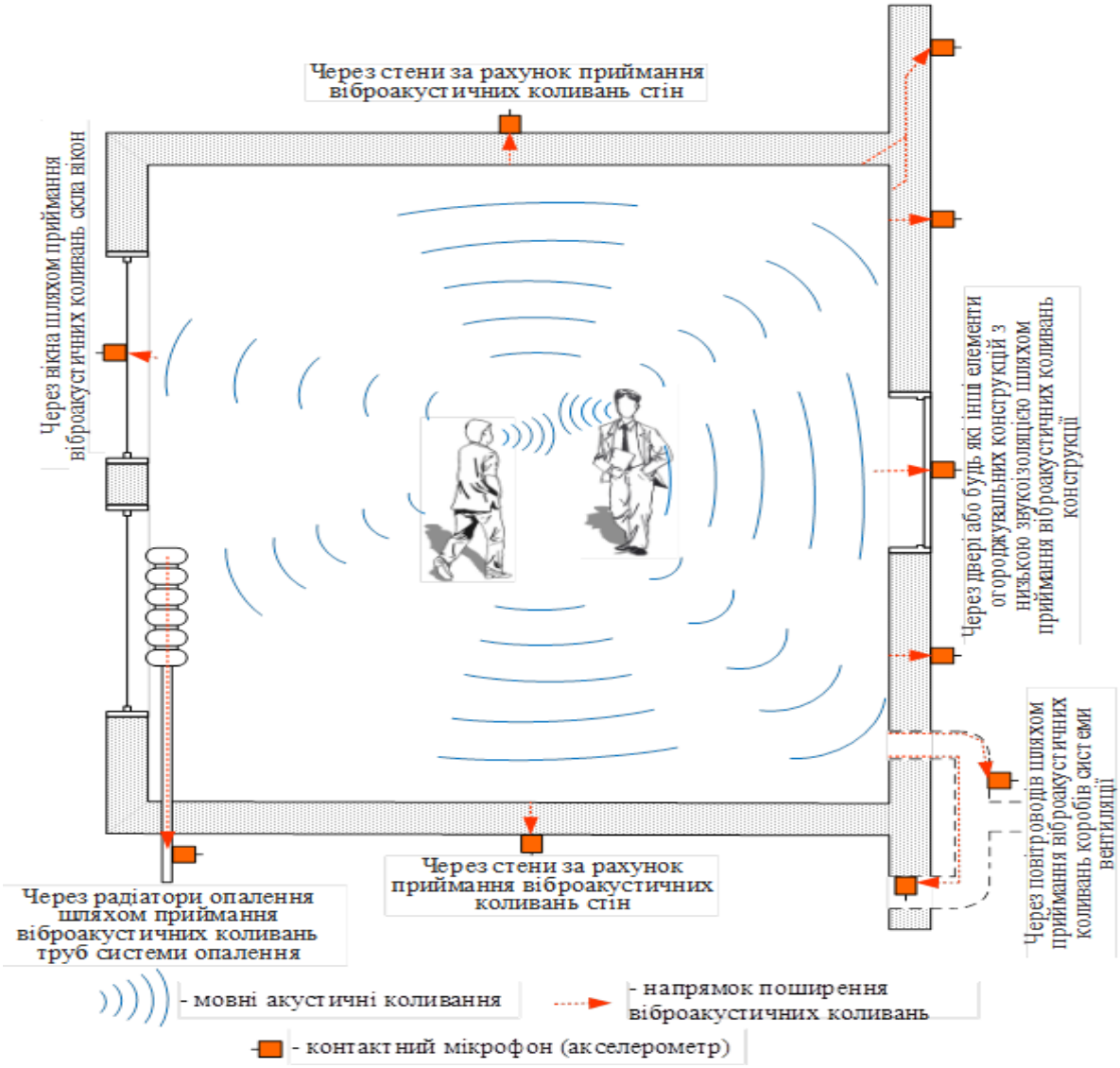

Рис.2.8. Віброакустичні канали витоку інформації

По віброакустичному каналу також можливо перехоплення інформації з використанням 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).

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 акустоэлектрического перетворення іноді називають «мікрофонним ефектом».

Перехоплення акустоэлектрических коливань в даному каналі витоку інформації здійснюється шляхом безпосереднього підключення до з'єднувальних ліній ДТЗС спеціальних високочутливих УНЧ.

Наприклад, підключаючи такі засоби до з'єднувальних ліній телефонних апаратів з електромеханічними викличними дзвінками, можна підслуховувати розмови, що ведуться в приміщеннях, де встановлені ці апарати.

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 акустоэлектрического перетворення акустичних сигналів в електричні. Промодульований сигнал відбивається від зазначених елементів і поширюється у зворотному напрямку або випромінюється.

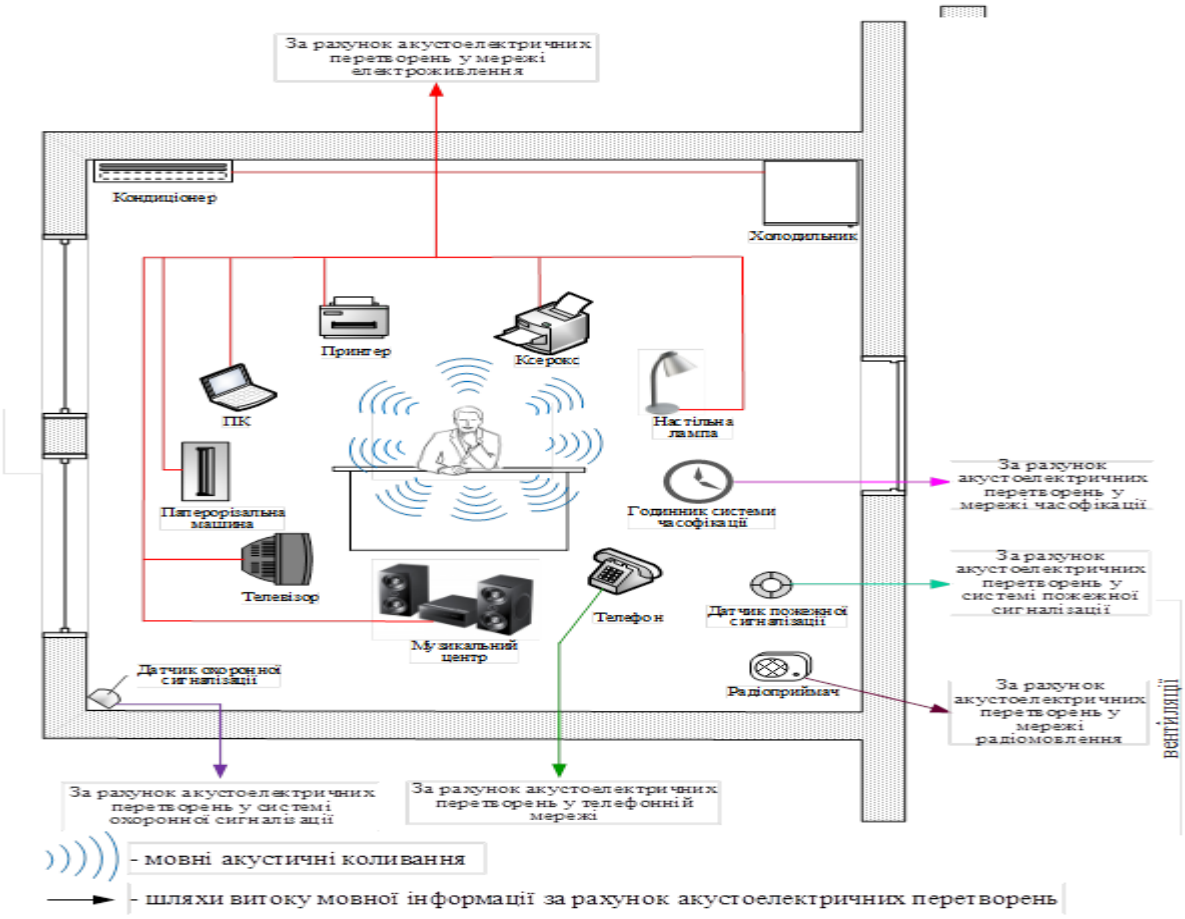

Рис.2.9. Канали витоку акустичної інформації за рахунок акустоелектричних перетворювань

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.

Для організації такого каналу є кращим використання дзеркального відбиття лазерного променя. Однак, при невеликих відстанях до поверхонь, що відбивають (порядку декількох десятків метрів) може бути використано дифузне віддзеркалення лазерного випромінювання.

Для перехоплення мовної інформації з даного каналу використовуються складні лазерні системи - «лазерні мікрофони», які працюють, як правило в ближньому інфрачервоному діапазоні довжин хвиль.

Параметричні утворюються 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 може бути організований і шляхом «високочастотного опромінення» приміщення, де встановлені закладні пристрої, що мають елементи, параметри яких (наприклад, добротність і резонансна частота об'ємного резонатора) змінюються під дією акустичного (мовного) сигналу.

При опроміненні приміщення потужним високочастотним сигналом в такому ЗП при взаємодії електромагнітного поля зі спеціальними елементами закладки (наприклад, чвертьхвильовим вібратором) 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 і прий

2.4. Організаційні заходи при проведенні нарад

В ході життєдіяльності підприємств, пов'язаної з використанням конфіденційної інформації, плануються і проводяться службові наради або засідання, на яких розглядаються або обговорюються питання конфіденційного характеру.

Прелатом обговорення можуть бути відомості, що становлять державну таємницю, питання конфіденційного характеру, торкаються тих, що проводяться підприємством науково - дослідницьких, досвідчено - конструкторських і інших робіт, передбачених його статутом, або комерційної сторони його діяльності.

Перераховані заходи можуть бути зовнішніми (за участю представників сторонніх організацій) або внутрішніми (до участі в них притягується тільки персонал цього підприємства). Рішення про проведення наради в усіх випадках приймає безпосередньо керівник підприємства або його заступник клопотанню керівника структурного підрозділу (відділу, служби), плануючого проведення цієї наради.

Заходи по захисту конфіденційної інформації в ході підготовки і доведення наради, що приймаються керівництвом підприємства (структурним підрозділом, організуючим нараду), мають бути як організаційними, так і організаційно - технічними.

Заходи по захисту інформації проводяться при підготовці, в ході проведення і після закінчення наради. У роботі керівництва і посадовців підприємства по захисту інформації при проведенні наради важливе місце займає етап планування конкретних заходів, напрямах на виключення просочування конфіденційної інформації і на її захист.

В цілях найбільш ефективного рішення завдань захисту інформації в тих, що розробляються організаційно - плануючих документах комплексно враховуються усі заходи, незалежно від їх змісту і спрямованості. Оскільки ці заходи мають бути пов'язані між собою за часом і місцю проведення.

Планування заходів по захисту інформації проводиться завчасно до початку наради і включає вироблення конкретних заходів, визначення відповідальних за їх реалізацію посадових осіб (структурних підрозділів), а також термінів їх здійснення. При плануванні наради передбачається така черговість розгляду питань, при якій буде виключено участь в їх обговоренні осіб, що не мають до них прямого відношення.

Найбільш актуальні з точки зору захисту інформації наради за участю представників сторонніх організацій (зовнішні наради), оскільки вірогідність просочування конфіденційної інформації при їх проведенні в порівнянні з нарадами, що проводяться у рамках одного підприємства (внутрішніми нарадами), значно вище.

Роботу по плануванню заходів в області захисту інформації, сторонніх організацій, що проводяться в ході наради за участю представників, очолює керівник підприємства, безпосередню участь в плануванні бере заступник, у веденні якого знаходяться питання захисту інформації на підприємстві. На заступника керівника підприємства також покладається загальна координація виконання спланованих заходів.

За відсутності в структурі підприємства цього посадовця, вказані завдання покладаються на керівника підрозділу (керівника служби безпеки).

План заходів по захисту інформації при проведенні наради за участю представників сторонніх організацій містить наступні основні розділи. Визначення складу учасників і їх сповіщення - порядок формування списку осіб, що залучаються до участі в нараді, і переліку підприємств, яким необхідно направити запити із запрошеннями; порядок підготовки і напряму таких запитів, формування їх змісту.

Підготовка службових приміщень, в яких планується проведення наради, робота по вибору службових приміщень і перевірці їх відповідності вимогам по захисту інформації; необхідність і доцільність вжиття додаткових організаційно-технічних заходів, спрямованих на виключення просочування інформації; устаткування робочих місць учасників наради, у тому числі засобами

автоматизації, на яких дозволена обробка конфіденційної інформації; порядок використання засобів звукопідсилення, кино- і відеоапаратури.

Визначення об'єму обговорюваної информации-порядок визначення переліку питань, що виносяться на нараду, і черговості їх розгляду, оцінки міри їх конфіденційності; виділення питань, до яких допускається вузьке коло осіб, що беруть участь в нараді.

Організація контролю за виконанням вимог по захисту информации-порядок, способи і методи контролю повноти і якості заходів, що проводяться, спрямованих на відвертання витоку і розголошування конфіденційної інформації, втрат розкрадань носіїв інформації; структурні підрозділи або посадовці, що відповідають за здійснення контролю; порядок і терміни представлення відповідальними посадовими особам доповідей про наявність носіїв конфіденційної інформації виявлених порушеннях в роботі по захисту інформації.

Якщо в ході наради використовуються відомості, що становлять державну таємницю, його учасники повинні мати допуск до них відомостям по відповідній формі.

При розгляді питань, віднесених до інших видів конфіденційної інформації, учасники наради повинні мати оформлене в уставленому порядку рішення керівника підприємства об допуск цієї категорії (цьому виду) інформації.

Посадовець, відповідальний за проведення наради, вказівці керівника підприємства (керівника підрозділу, організуючого нараду) формує список осіб, що беруть участь в нараді.

У списку вказують прізвище, ім'я, по батькові кожного учасника, його місце роботи і посаду, номер допуску до відомостей що становить державну таємницю, або номер рішення рук водія про допуск до іншої конфіденційної інформації, і міра питань наради, до обговорення яких допущений учасник. При необхідності в списку можуть вказуватися і інші відомості.

Підготовлений список учасників узгоджується з таємно - режимним підрозділом (службою безпеки) підприємства наради і затверджується керівнику цього підприємства, що дав дозвіл на проведення наради.

Включені в список учасники наради проходять в службові приміщення, в яких воно проводиться, пред'являючи співробітникам служби охорони (служби безпеки) документ, що засвідчує особу. Прохід учасників наради в ці приміщення може бути організований по пропусках, выдаваемы їм виключно на період проведення наради і що відрізняється від інших використовуваних підприємством-організатором пропусків.

Учасники наради мають право відвідування тільки тих службових приміщень, в яких обговорюватимуться питання, до яких ці учасники мають безпосереднє відношення.

Перевірку документів, що підтверджують наявність у учасників наради допуску до відомостей, що становлять державну таємницю, і дозволів на ознайомлення з конфіденційною інформацією здійснює служба безпеки підприємства-організатора наради.

Перевірка службових приміщень та огляд засобів інформації і тд.

2.5. Технічні заходи захисту акустичної інформації в кімнаті для нарад

Для повного захисту акустичної інформації розглянемо ряд запитань та відповідей.

А саме у кімнаті для проведення нарад можна підкреслити наступні канали витоку акустичної інформації з приміщення:

- Вікно;
- Стіни;
- Підлога, стеля;
- Двері;
- Батарея центрального опалення.
- Компютери

Акустична захист приміщення для нарад є особливо важливою, оскільки при проведенні наради акустична інформація відноситься до найбільш конфіденційною.

Для захисту мовної інформації застосовується комплекс активних і пасивних засобів:

– Енергетичне приховування шляхом:
– Звукоізоляції акустичного сигналу;
– Звукопоглинання акустичної хвилі;
– Глушіння акустичних сигналів;
– Зашумлення приміщення або твердого середовища розповсюдження іншими широкосмуговими звуками, які забезпечують маскування акустичних сигналів.
– Виявлення, локалізація і вилучення заставних пристроїв.

До пасивних методів відноситься звукоізоляція і екранування.

В умовах наради не варіант зменшувати гучність звуку, тому для захисту такої інформації слід застосовувати звукоізоляцію, звукопоглинання і глушіння звуку.

Звукоізоляція локалізує джерела акустичних сигналів у замкнутому просторі. Основна вимога до звукоізоляції: не повинно перевищувати максимально допустимі значення, що виключають добування інформації зловмисниками.

Стосовно до даного об'єкту, необхідна звукоізоляція віконних прорізів дверей, а також використання звукоізолюючих покриттів.

Технічні заходи по захисту інформації

Наступні три головні напрями включають технічні заходи по захисту інформації :

– знаходження, локалізація і усунення заставних пристроїв для прослуховування;
– створення ситуацій, при яких відбувається пригнічення небезпечних сигналів з мовною інформацією з метою виключення просочування конфіденційної інформації;

– застосування усіх можливих процедур по поліпшенню звукоізоляції приміщення для переговорів.

Переслідуючи цілі недопущення підслуховування за допомогою заставних пристроїв перед розглядом тих робіт, які слід провести потрібно проводити "чищення" приміщення, вона проводиться співробітниками служби безпеки організації, недоцільно запрошувати співробітників спеціалізованих організацій, для вищеназваних цілей. Далі переговорна кімната опечатується, допуск сторонніх осіб неможливий, або при гострій необхідності це слід робити тільки з представником співробітника служби безпеки організації.

Слід провести наступні заходи по захисту від заставних пристроїв в переговорній кімнаті:

– перевіряти приміщення і в робочий і в неробочий час на предмет знаходження в переговорній кімнаті радіозакладок;
– вести оперативну роботу по перевірці обстановки під час проходження конфіденційної розмови на випадок виявлення радіозакладок, які можуть знаходиться і на тілі учасника переговорів, і в складках його одягу;
– вести оперативну роботу по перевірці обстановки на випадок знову встановлених радіозакладок;
– слід не лише виявити наявність закладки, але і встановити з точністю її місцезнаходження, для подальшого її вилучення;
– якщо сталося виявлення радіозакладки під час конфіденційної розмови, то слід відразу припинити нараду і почати шукати зловмисника, ця ситуація поза сумнівом створить неділову обстановку для учасників конфіденційної розмови і викличе напруженість у учасників і недовіру один до одного, а також кине тінь на можливо безневинного учасника наради. Ці заходи можуть насторожити зловмисника, який може позбавитися від закладки.
– після закінчення наради слід обстежувати підозрюваного, застосувавши апаратуру, яка дозволить максимально точно визначити

місце, в якому знаходиться радіозакладка, а також її потенційного володаря.

Переговорну кімнату слід захистити за допомогою безпосереднього виявлення і усунення радіозакладки, а також необхідно створити активні радіоелектронні перешкоди, які будуть в діапазоні частоти закладки.

Усунення закладки нескладно виконати в той час, коли наради не проводяться, інакше, доцільне використання методу створення активних радіоелектронних перешкод, для виключення просочування конфіденційної інформації, яка обговорюється на нараді.

З метою виявлення працюючого диктофона, який схований на тілі учасника конфіденційної розмови, слід застосовувати офісне облаштування PRD 018, в комплект якого входить 18 датчиків, розташовані під стільницею столу в переговорній кімнаті. Облаштування PRD 018 локалізує місцезнаходження диктофона, і з точністю показує володаря диктофона.

Застосування усього комплексу вищеперелічених технічних і організаційних заходів по захисту конфіденційної інформації, забезпечить необхідний рівень захисту звукової інформації, яка озвучується в переговорній кімнаті.

При проведенні наради зменшення гучності мови недоречне, тому захищаючи цю інформацію необхідно застосовувати звукоізоляцію, звукопоглинання і глушення звуку. Звукоізоляція і екранування відноситься до пасивних методів захисту конфіденційної інформації.

Пасивні способи зменшують рівень небезпечних сигналів, активні - підвищують рівень перешкод.

Для переговорної кімнати украй важлива звукоізоляція, яка локалізує джерела звукових сигналів в замкнутій переговорній кімнаті, головна умова до звукоізоляції наступна: за межами кімнати співвідношення сигналів/перешкода не може бути більша за максимально допустимі показники з метою виключення просочування конфіденційної інформації до зловмисників.

Самі уразливі для просочування конфіденційної інформації місця переговорної кімнати це двері і вікна, тому як двері мають куди більше менший,

якщо порівнювати з іншими спорудами, що захищають, поверхневою щільністю полотен, а також проміжки і щілини не ущільнюються або важко ущільнюються. Звичайні двері не можуть бути використані в приміщенні, де проводяться конфіденційні розмови, тому як вони не проходять за тими вимогами, які мають бути по захисту інформації в приміщеннях від прослуховування.

Двері слід застосовувати спеціалізовані, або проводити максимально можливі заходи по додатковій шумоізоляції, необхідно застосувати додаткові ущільнюючі прокладення по усьому периметру дверей, ці прокладення здатні збільшити шумоізоляцію дверей до десяти децибел, але тут варто враховувати відсоток зносу цих шумопоглинаючих прокладень, оскільки з часом вони стають тонше і твердіше, що знижує їх ефективність.

У зв'язку з вищесказаним для захисту конфіденційної інформації необхідно використати або спеціально розроблені двері з шумоізоляцією або подвійні двері, між якими знаходиться тамбур. Також доцільно використати полотна дверей, що більше обважнюють плюс бажано оббити їх повстяним матеріалом, і звичайно ж використати спеціальні прокладення, які при ущільненні дверей дають хорошу звукоізоляцію.

На малюнку 1 продемонстрована конструкція дверей з підвищеною звукоізоляцією. При організації тамбурів, звукоізоляцію підвищить ущільнення щілин над підлогою за відсутності порогів, а також облицювання внутрішніх поверхонь тамбура звукопоглинальними покриттями.

При проектуванні кімнат з вікнами, вікна повинні займати, за умовами освітленості, не малі простори, а як вже було сказано вище - вікна це хороший провідник звукових хвиль для спеціальної підслуховуючої техніки, втім і двері займають достатнє місце в переговорній кімнаті і, є хорошим каналом для витоку конфіденційних даних.

Стандартні двері не задовольняють вимогам щодо захисту інформації в приміщеннях від прослуховування, тому слід застосовувати двері з підвищеною звукоізоляцією, шляхом застосування додаткових ущільнюючих прокладок по периметру притвору дверей. Застосування ущільнювальних прокладок підвищує

звукоізоляцію дверей на 5-10 дБ. Проте в результаті експлуатації дверей, гумові прокладки зношуються, стираються, тверднуть. Ці чинники ведуть до порушення звукоізоляції.

Вікна, що займають за умовами освітленості досить великі площі огороджувальних конструкцій приміщень, також як і двері, є елементом середовища поширення потенційних каналів витоку інформації.

З наведених даних випливає, що звукоізоляція одинарного скління порівнянна зі звукоізоляцією одинарних дверей і недостатня для надійного захисту інформації в приміщенні. Таким чином, для підвищення звукоізоляції раціонально використання вікон з заскленням в роздільних палітурках з шириною повітряного проміжку більше 200 мм або з потрійним комбінованим склінням.

Крім вікон і дверей, витік акустичної інформації в розглянутому приміщенні можлива за огрівальним батареєю і вентиляцією. На вентиляційні отвори необхідно встановити екрани, таким чином, щоб екран виготовлений, наприклад, з алюмінію і оббитий всередині пінопластом, був розміром на кілька сантиметрів більше вентиляційного отвору і був встановлений на відстані 10 см від отвору.

Для запобігання витоку інформації з опалювальних систем необхідне використання екранування батарей. Екрани виготовляються в основному з алюмінію і покриваються зверху шаром пінопласту або якого-небудь іншого ізолюючого матеріалу.

Звукоізоляцію в приміщенні можна підвищити застосувавши звукопоглинальні матеріали.

Так як для досягнення найбільшої ефективності зниження рівня небезпечного сигналу площа акустичної обробки приміщень повинна становити не менше 60%, то для захисту приміщення найкраще застосувати для оздоблення стін і стелі панелі з пінопласту (з зазором 3 мм).

Для більш надійного захисту інформації рекомендується установка підвісної стелі (з обробкою панелями з пінопласту).

Крім пасивних методів, розглянутих вище, доцільно застосування та активних методів, наприклад, генератори шуму.

Одним з поширених генератором шуму є пристрій «Поріг-2М» НІІСТУ МВС Росії, призначений для захисту службових приміщень від підслуховування за допомогою радіотехнічних, лазерних, акустичних та інших засобів. Дозволяє захищати від витоку інформації через стіни, вікна, труби опалення та водопостачання, вентиляційні колодязі і т. п.

Пристрій працює в режимі «чергового прийому», тобто включається тільки в разі, якщо в захищеному приміщенні починається розмова.

Іншим, аналогічним за призначенням пристроєм, є виріб «Кабінет» СНВО «Елерон», призначене для запобігання прослуховування мовної інформації за межами приміщення, що захищається. Принцип дії заснований на створенні маскуючого вібраційного шуму в огороджувальних конструкціях і акустичного шуму в об'ємі приміщення і поза ним.

У цілому, як показує практика, застосування описаних генераторів шуму не порушує комфортності при роботі в захищеному з їх допомогою приміщенні.

Однак, з точки зору повної комфортності роботи людини в приміщенні, на думку фахівців, є комплекс віброакустичного захисту «Барон», в якому реалізовані можливості з налаштування помехового сигналу. Наявна в комплексі система налаштування спектра перешкоди (еквалайзер) дозволяє забезпечити необхідне перевищення рівня перешкоди над рівнем мовного сигналу при мінімальному впливі на людей, тобто створити оптимальну перешкоду. Використання саме цього генератора рекомендується для даної кімнати для нарад.

Технічні заходи щодо захисту інформації включають в себе три основних напрямки:

- виявлення, локалізація і вилучення заставних пристроїв;
- придушення небезпечних сигналів з мовної інформації;
- підвищення звукоізоляції приміщення.

Для запобігання підслуховування за допомогою закладних пристроїв перед обговоренням комплексних робіт необхідно проведення поглибленої «чистки» приміщення. Вона повинна проводиться фахівцями служби безпеки організації.

Запрошення співробітників спеціалізованих організацій, для проведення подібних заходів небажано.

Після проведення «чистки» приміщення має опечатуватися і допуск до нього повинен бути дозволений лише в супроводі працівника служби безпеки.

Для забезпечення захисту від закладних пристроїв у кімнаті для проведення нарад необхідно:

– Не тільки перевіряти приміщення в неробочий час на предмет залишених у ньому радіозакладок, але також вести оперативну перевірку обстановки під час проведення конфіденційного наради на предмет виявлення радіозаставних пристроїв, що знаходяться на тілі людини і в предметах одягу або щойно встановлених;

– Необхідно не тільки виявлення наявності закладки, але івстановлення з максимально можливою точністю її місцезнаходження, з метою подальшого її вилучення;

– У разі виявлення закладку під час проведення наради, недоцільно негайно припиняти його і починати займатися пошуком зловмисника. Це може створити неділової атмосферу в учасників наради, викликати напруженість підозріліть одне до одного, кинути тінь на невинну людину. Це також може насторожити зловмисника і спровокувати його на те, щоб позбутися від закладки. У цьому випадку, необхідне застосування активних заходів захисту просторового зашумлення кімнати.

Після закінчення наради необхідно провести безпосереднє обстеження підозрюваного. Саме для цього необхідне застосування апаратури, яка дозволяє максимально точно визначити місцезнаходження закладки та її потенційного власника.

Захист від радіозакладок можлива шляхом безпосереднього вилучення закладку або створення активних радіоелектронних перешкод в діапазоні частот закладки.

Вилучення закладки не складає труднощів поза часом проведення нарад. В іншому ж випадку, доцільно використання методу створення активних радіоелектронних перешкод.

Для виявлення працюючого диктофона, захованого на тілі одного з учасників наради, найбільш ефективно офісний пристрій PRD 018, який комплектується вісімнадцятьма датчиками, які розміщуються під стільницею стола в кімнаті. Цей пристрій локалізує місцезнаходження диктофона, а відповідно і вказує його володаря.

Зловмисник може отримати конфіденційну інформацію через вікна. У уникнення витоку акустичної інформації за допомогою лазерного пристрою знімання інформації з скла, за допомогою закладних пристроїв, а також з використанням спрямованих мікрофонів, рекомендується покрити вікна металізованою плівкою.

Застосування всього комплексу перерахованих організаційних і технічних заходів із захисту, забезпечить належний рівень захисту акустичної інформації, що циркулює в кімнаті для проведення наради.

Забезпечення безпеки під час проведення нарад за участю представників сторонніх організацій має ряд особливостей, викликаних великим збитком у разі витоку інформації, різнорідністю складу і відносно великою кількістю учасників, високим ступенем концентрації та узагальнення відомостей, великою ймовірністю проносу диктофонів і радіозакладок учасниками наради.

Дані особливості пред'являють підвищені вимоги до підготовки приміщення, способів і засобів захисту інформації в ході наради.

На підставі результатів проведеної роботи можна зробити наступні висновки:

інформацію, яка циркулює в розглянутому приміщенні, можна розділити на мовну і на магнітних носіях.

у якості основних загроз безпеки інформації під час проведення наради виступають:

– підслуховування і несанкціонована запис мовної інформації за допомогою закладних пристроїв, систем лазерного підслуховування, стетоскопів, диктофонів;

– реєстрація на неконтрольованої території за допомогою радіомікрофонів учасниками, які виконують агентурне завдання;

– перехоплення електромагнітних випромінювань при роботі звукозаписних пристроїв та електроприладів.

Для запобігання витоку інформації пропонується комплекс організаційних і технічних заходів перед проведенням наради і в ході наради.

У якості основних організаційних заходів рекомендується:

– перевірка приміщення перед проведення наради, з метою оцінки стану забезпечення безпеки інформації;

– Управління допуском учасників наради до приміщення;

– Організація спостереження за входом в вибраного приміщення і навколишнім оточенням в ході проведення наради.

– Основними засобами забезпечення захисту акустичної інформації при проведенні наради є:

– Установка різних генераторів шуму, моніторинг приміщення на предмет наявності закладних пристроїв, звукоізоляція.

– В якості основних технічних засобів захисту інформації були запропоновані наступні заходи:

– проведення «чистки» приміщення на предмет наявності закладок перед проведенням нарад;

– використання килимових покриттів для підвищення звукоізоляції;

– оббивка звукопоглинаючим матеріалом дверей приміщення;

закладення наявних у вікнах щілин звукопоглинаючим матеріалом.

Отже, ля захисту інформації в даному об'єкті, доцільно застосовувати спеціально розроблені звукоізолюючі двері, або подвійні двері з тамбуром. При цьому, доцільно застосувати обтяжені полотна дверей, оббити їх матеріалами з шарами вати або повсті, використовувати додаткові ущільнюючі прокладки,

валики і так далі. При організації тамбурів дверей, звукоізоляцію підвищить ущільнення щілин над підлогою при відсутності порогів, а також облицювання внутрішніх поверхонь тамбура звукопоглинальними покриттями.

3 СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ З ВИКОРИСТАННЯМ ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ВІД ВИТОКУ ПО АКУСТИЧНОМУ КАНАЛУ

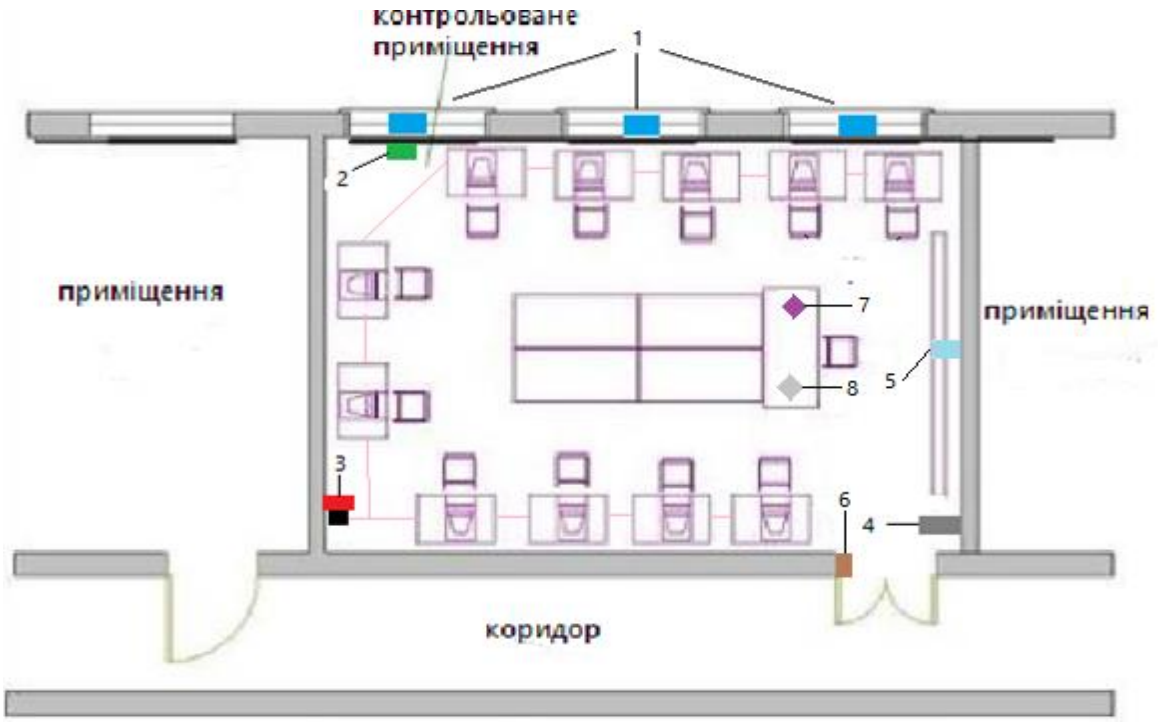

Рис.3.1. План захищеного приміщення

Для захисту приміщення доцільно використовувати

1 – віброакустична система захисту на вікна, рамки

2 – віброакустична випромінювальна система захисту на системи опалення і стіни

3 – генератор шуму по мережі електроживлення і заземлення

4 – генератор шуму в акустичному діапазоні

5 – генератор електромагнітного шуму

6 – акустичний випромінювач системи захисту інформації в міждверному просторі

7 – акустичний сейф для мобільних телефонів

8 – пристрій захисту телефонних перемовин

Для захисту приміщення рекомендованим є використання таких засобів технічного захисту:

Комплекс віброакустичного захисту "БАРОН"

Рис.3.2. Комплекс «Барон»

Комплекс віброакустичного захисту "БАРОН" призначений для захисту об'єктів інформатизації 1,2 та 3 категорії та протидії технічним засобам перехоплення мовної інформації (стетоскопи, спрямовані і лазерні мікрофони, виносні мікрофони) по віброакустичними каналах (наведення мовного сигналу на стіни, підлогу, стелю приміщень, вікна, труби опалення, вентиляція
і повітряні зазори

Комплекс віброакустичного захисту "БАРОН" має чотири канали формування перешкод, до кожного з яких можуть підключатися віброперетворювачі п'єзоелектричного або електромагнітного типу, а також акустичні системи, що забезпечують перетворення електричного сигналу, який формується приладом, в механічні коливання в огороджувальних конструкціях приміщення, а також в акустичні коливання повітря.

Переваги комплексу "Барон":

– повністю цифрове управління;
– інтелектуальне меню, гнучка система конфігурацій

– можливість формування помехового сигналу від різних внутрішніх ізовнішніх джерел а також їх комбінацій

Внутрішні джерела - генератор шуму, фонемний Клонер, призначений для синтезу мовоподібної, оптимізованих для захисту мовної інформації конкретних осіб перешкод, шляхом клонування основних фонемний складових їх мови. За рахунок їх мікшування по кожному каналу значно зменшується ймовірність очищення перешкоди сигналу. Крім того, наявність лінійного входу дозволяє підключати до комплексу джерела спеціального по-
мехового сигналу підвищеної ефективності;

– кожен канал приладу має власний незалежний генератор шуму аналогового типу і фонемний Клонер, що дозволяє виключити можливість компенсації помехового сигналу засобами перехоплення мовної інформації за рахунок спеціальної обробки, в тому числі і кореляційними методами при багатоканальному зніманні кількома датчиками;

– одним приладом можна захистити приміщення великої площі різного призначення (конференц-зали тощо);

– можливість регулювання спектра помехового сигналу для підвищення ефективності наведеного помехового сигналу з урахуванням особливостей використовуваних вібро-акустичних випромінювачів і захищаються поверхонь (5 смуговий цифровий еквалайзер);

– наявність чотирьох незалежних вихідних каналів з роздільними регулюваннями (для оптимальної настройки помехового сигналу) для різних поверхонь, що захищаються і каналів витоку. Досягнення максимальної ефективності придушення при мінімальному паразитному акустичному шумі в приміщенні, що підлягає за рахунок вищеперелічених можливостей настройки комплексу;

– вбудовані засоби контролю ефективності створюваних перешкод: контрольний динамік для експертної оцінки якості створюваної перешкоди і низькочастотний чотирьохканальний п'ятиполосний аналізатор спектру, який працює з вихідними сигналами всіх 4 каналів, що володіє широким динамічним

діапазоном, що дозволяє ефективно безперервно проводити контроль перешкод будь-якого рівня, що створюються в кожному з каналів у всьому частотному діапазоні роботи приладу;

– можливість підключення до кожного вихідного каналу різних типів вібро-і акустичних випромінювачів і їх комбінацій за рахунок наявності низкоомного і високоомного виходів. Це також дозволяє використовувати комплекс для заміни морально застарілих або вийшли з ладу джерел помехового сигналу в уже розгорнутих системах віброакустичного захисту без демонтажу і заміни

– встановлених віброакустичних випромінювачів;

– наявність системи бездротового дистанційного включення комплексу.

В комплекс входе:

– віброгенератор «Барон»;

– компакт-диск з програмним забезпеченням;

– кабель для запису сформованих перешкод в Клонер через послідовний порт ПЕОМ;

– модуль дистанційного керування по радіоканалу (опція);

– пульт дистанційного керування по радіоканалу (опція);

– мережевий шнур;

– технічний опис та інструкція з експлуатації.

Технічні параметри

– Додатково може бути укомплектований пристроями контролю ефективності перешкод "Барон-К", "Барон-ДК", пристроями дистанційного включення "Барон-В".

– "Барон-В" - пристрій дистанційного включення віброгенераторів типу "Барон". Забезпечує включення (виключення) віброгенераторів за допомогою власних органів управління, а також в якості інтерфейсного обладнання для подачі команд на включення (виключення) віброгенераторів з керуючої ПЕОМ.

Забезпечує дистанційне керування дванадцятьма віброгенератори. Конструктивно виконаний у вигляді модуля для монтажу в RACK-стійки (шафи).

– "Барон-К" - пристрій контролю ефективності вібраційних перешкод, створюваних віброакустичними генераторами типу "Барон" або аналогічної апаратурою. Забезпечує попередження про зниження рівня вібраційного перешкоди на огороджувальної конструкції приміщення, що підлягає нижче допустимого в результаті виходу з ладу вібраторів, генератора перешкод, зміни навколишніх умов. До одного комплексу віброакустичного захисту «Барон» можна підключити до 10 пристроїв "Барон-К".

– "Барон-ДК" - віддалений комунікатор для контролю ефективності вібраційних перешкод, створюваних віброакустичними генераторами типу "Барон" або аналогічної апаратурою. Забезпечує попередження про зниження рівня вібраційного перешкоди на огороджувальної конструкції приміщення, що підлягає нижче допустимого в результаті виходу з ладу вібраторів, генератора перешкод, зміни навколишніх умов. До "Барон-ДК" підключаються до дванадцяти датчиків (пристроїв контролю типу "Барон-К"), які здійснюють знімання вібраційних сигналів з контрольованих огороджувальних конструкцій, їх попередню обробку і посилення.

• "Копійка" - вібраційний випромінювач на скло.

Рис.3.3. "Копійка"

• "Молот" - вібраційний випромінювач на стіну.

Рис.3.4. "Молот"

• "Серп" - вібраційний випромінювач на раму вікна.

Рис.3.5. "Серп"

Генератор шуму "БАЗАЛЬТ - 5ГЕШ" призначений для захисту об'єктів від витоку інформації по каналах побічних електромагнітних випромінювань персональних комп'ютерів , робочих станцій комп'ютерних мереж і комплексів.

Забезпечує захист за допомогою придушення можливих побічних електромагнітних випромінювань за рахунок створення потужного просторового електромагнітного поля шуму (ЕМПШ) .

Пристрій являє собою генератор , що формує і випромінюючий в навколишній простір у широкому діапазоні частот ЕМПШ . Один генератор забезпечує маскування (захист) інформації пристроїв обчислювальної техніки , розміщеної в приміщенні площею ~ 40 м2.

У пристрої передбачена можливість автоматичної звукової та візуальної сигналізації в разі виникнення неполадок у його роботі.

Рис.3.6. "БАЗАЛЬТ - 5ГЕШ"

ТЕХНІЧНІ ПАРАМЕТРИ:

– Діапазон робочих частот, МГц 0,1-1000;

– Значення спектральної щільності напруженості магнітного й електричного компонентів нормованого електромагнітного поля шуму генератора на відстані 1 м, дБ 45-80;

– Ентропійний коефіцієнт якості електромагнітного поля шуму генератора (не менше) 0,8;

– Електроживлення, 50 Гц 220 В;

– Споживана потужність, Вт 6;

– Габарити, мм 700х70х130;

Висновки по розділу. На підставі попередніх досліджень розроблена система захисту акустичної інформації на об’єкті інформаційної діяльності від витоку акустичним каналом.

ВИСНОВКИ

Захист мовної інформації є дуже важливою задачею у комплексі заходів по забезпеченню інформаційної безпеки. Для отримання мовної інформації зловмисник може використовувати широкий арсенал засобів акустичної розвідки, що дозволяє перехоплювати мовну інформації по прямому акустичному, віброакустичному, електроакустичному та ін. каналах. Тому дослідження сучасних методів та засобів захисту інформації має практичне значення та є актуальними.

В даній дипломній роботі було проведено дослідження вимог до захисту інформації. Встановлена необхідність захисту інформації з грифом «таємно» та «цілком таємно» від витоку акустичним каналом. В результаті дослідження встановлено, інформація, що озвучується на нарадах є найбільш цінною. Витік інформації акустичним каналом з об’єкта інформаційної діяльності здійснюється шляхом безперервного прослуховування та прослуховування за допомогою технічних засобів. Встановлено що для захисту інформації на об’єкті інформаційної діяльності від витоку по акустичному каналу застосовуються пасивні та активні методи. Пасивні методи базуються на інженерних заходах, а активні використовують технічні

Встановлено,що для отримання інформації несанкціонованим доступом через акустичний канал найчастіше використовують радіозакладки, направлені мікрофони, стетоскопи та акустоперетворювачі. Для захисту інформації використовують комплекси віброакустичного захисту, генератори шуму в акустичному діапазоні і ультразвукові генератори. Надані основні правила для організаційних і технічних заходів при проведенні нарад

На основі отриманих при дослідженні даних було виконано поставлену мету дипломної атестаційної роботи, а саме розроблено систему захисту інформації від витоку по акустичному каналу на об'єкті інформаційної діяльності.

ПЕРЕЛІК ПОСИЛАНЬ

Електронні ресурси

1. WEB-сайт: www.tzi.com.ua
2. WEB-сайт: http://zakon3.rada.gov.ua
3. https://webcache.googleusercontent.com/search?q=cache:8HiwJvQQss0J:https://manager.bobrodobro.ru/16310+&cd=9&hl=ru&ct=clnk&gl=ua

Книги

4. Хорошко В. А., Чекатков А. А. “Методы и средства защиты информации” Юниор 2003г
5. Ярочкин В.И. Інформаційна безпека. Підручник для студентів вузів /3е изд. – М.: Академічний проект: Трікста, 2005. – 544 з.
6. Барсуков В.С. Сучасні технології безпеки / В.С. Борсуків, В.В.Водолазській. – М.: Нолідж, 2000. – 496 з., мул.
7. Зегжда Д.П. Основи безпеки інформаційних систем / Д.П. Зегжда, А.М.Івашко. – М.: Гаряча лінія – телеком, 2000. – 452 с., мул.
8. Комп’ютерна злочинність і інформаційна безпека А.П. Леонов[ідр.]; під заг. Ред. А.П. Леонова. – Мінськ: АРІЛ, 2000. – 552 с.
9. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. М.: Российск. гос. гуманит. ун-т, 2002.
10. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. - 320 с.
11. Абалмазов Э.И. Направленные микрофоны: мифы и реальность //«Специальная техника» №4, 1996 г.
12. Иксар В. Современные способы перехвата информации. «Специальная техника» №2 1998 г.
13. Системы и комплексы технических средств местоопределения подвижных объектов. «Специальная техника», №3, 1998 г.

14. Петров Н.Н. Местоопределение подвижных объектов на основе спутниковых навигационных систем. // Журнал «Специальная техника», №1, 1999.

15. Оленин Ю.А., Петровский Н.П. Системы безопасности. «Специальная техника», №29 1999г.

16. Ларин И. Быстроразвертываемые охранные системы. «Специальная техника», №4, 2000.

17. Введенский Б.С. Современные системы охраны периметров. «Специальная техника», №4, 1999.

18. Ллойд Дж. Системы тепловидения. М.: Мир, 1978.

19. Андреев С.П. ИК-пассивные датчики охранной сигнализации. Источник: журнал «Специальная техника» №1, 1998.

20. Барсуков В.С., Марущенко В.В., Шигин В.А. Интегральная безопасность: Информационно-справочное пособие. - М.: РАО «Газпром», 1994. - 170 с.

21. Специальная техника: Каталог. - М.: Гротек, 1996. - 83 с.

22. Специальная техника: Каталог. - М.: НПО «Защита информации», 1996. - 56 с.

23. Специальная техника: Каталог. - М.: Прогресстех, 1996. - 79 с.

24. А.А. Хорев. Оценка эффективности защиты вспомогательных технических средств. // Специальная техника. - № 2, №3. - 2007.

25. Анюхин С.Г. Радиоволновые извещатели для охраны периметра. «Системы безопасности» №5 (59), 2004 г.

26. Зайцев А.П., Шелупанов А.А. Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации. Изд. Томского гос. ун-та систем управления и радиоэлектроники, 2004. - 197с.

27. Волков В.Г. Наголовные приборы ночного видения. Источник: журнал «Специальная техника», №5, 2002.

28. Доценко С.М. Безопасность оптоволоконных кабельных систем //«Конфидент», №6, 1999.

29. Бландова Е.С. Помехоподавляющие изделия. Рекомендации по выбору и применению // Источник: журнал «Специальная техника», №2, 2001.

30. Шокало В.М. Поля і хвилі в системах технічного захисту інформації / В.М. Шокало, В.А. Усін, Д.В. Грецьких, В.О. Хорошко, Л.П. Крючкова / ХНУРЕ Колегіум, м. Харків. 2013. С. 450.

31. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об’єктах інформаційної діяльності / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін / ДУТ, м. Київ. 2020. С. 126.

32. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації / О.А. Лаптєв / ДУТ, м. Київ. 2020. С. 326.

33. Крижановський В.Г. Підслуховування NFC-зв`язку на частотах вищих гармонік / В.Г. Крижановський, С.П. Сергієнко, Д.В. Чернов, В.В. Крижановський // Радіотехніка, вип. 204, 2021. - С. 99-104.

34. Сергієнко С.П. Ефективні режими роботи радіозакладних пристроїв для потайного знімання інформації у полі шумових завад / С.П. Сергієнко, В.Г. Крижановський, Д.В. Чернов, Л.В. Загоруйко // Радіотехніка, вип. 205, 2021. - С. 169-174.