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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія ефективного захисту акустичної інформації на режимних об’єктах»

на здобуття освітнього ступеня магістра
зі спеціальності __125 - _Кібербезпека та захист інформації»_____
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

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

Виконав: здобувач вищої освіти групи СЗДМ 61
Андрій ОПАЛЬКО

Керівник:__ Ігорь ІВАНЧЕНКО_____
к.т.н., доцент (Ім’я, ПРІЗВИЩЕ)

Рецензент:_____
(Ім’я, ПРІЗВИЩЕ)

Київ 2025

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

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність __Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУРОБОТУ

_____Опалько Андрію Едуардовичу _____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Технологія ефективного захисту акустичної інформації на режимних об'єктах»
керівник кваліфікаційної роботи ____Ігорь ІВАНЧЕНКО к.т.н., доцент_____

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

3. Вихідні дані до кваліфікаційної роботи:
__Загрози акустичній інформації на об'єктах інформаційної діяльності_____
__Методи акустичної інформації_____
__Засоби захисту акустичної інформації _____

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. __Інформаційній безпека об'єкту інформаційної діяльності_____
2. __Методи та засоби захисту акустичної інформації_____
3. __Підвищення ефективності захисту акустичної інформації на режимних об'єктах_____

5. Перелік графічного матеріалу: __Презентаційний матеріал на 18 слайдах_____

6. Дата видачі завдання _____20.10.2024 ___ _____

КАЛЕНДАРНИЙ ПЛАН

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

Здобувач вищої освіти _____ _Андрій ОПАЛЬКО_____
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ __Ігорь ІВАНЧЕНКО_
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи: 73 стор., 16 рис., 10 таблиць, 18 джерел.

Об'єкт дослідження – Процес захисту інформації.

Предмет дослідження – Захист акустичної інформації.

Мета роботи – Розробка технології ефективного захисту акустичної інформації на режимних об'єктах.

Методи дослідження – системний аналіз, чисельні методи.

У роботі розглянуто загрози акустичній інформації на режимних об'єктах. Проаналізовано активні та пасивні методи та засоби захисту інформації.

Розроблено технологію ефективного захисту акустичної інформації.

Галузь використання – інформаційна безпека.

Апробація:

Козеренко Д.О., Опалько А.Е., Адаптивний захист акустичної інформації. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.15 - 17.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

БЕЗПЕКА, ЗАГРОЗИ ІНФОРМАЦІЇ, ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АКУСТИЧНИЙ КАНАЛ, ЗАСОБИ ЗАХИСТУ, АКТИВНІ МЕТОДИ ЗАХИСТУ, ПАСИВНІ МЕТОДИ ЗАХИСТУ, СТЕТОСКОП.

ABSTRACT

Text part of the master's qualification work: 73 pages, 16 figures, 10 tables, 18 sources.

Object of research – Information protection process.

Subject of research – Acoustic information protection.

Purpose of work – Development of technology for effective protection of acoustic information at regime facilities.

Research methods – system analysis, numerical methods.

The paper considers threats to acoustic information at regime facilities. Active and passive methods and means of information protection are analyzed.

A technology for effective protection of acoustic information is developed.

Field of application – information security.

Approbation:

Kozerenko D.O., Opalko A.E., Adaptive protection of acoustic information. All-Ukrainian scientific and practical conference: Current problems of security of information and telecommunication systems. Kyiv, November 3, 2024, Kyiv: RVC DUIKT. – 024. P.15 - 17.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

SECURITY, THREATS TO INFORMATION, OBJECT OF INFORMATION ACTIVITY, ACOUSTIC CHANNEL, MEANS OF PROTECTION, ACTIVE PROTECTION METHODS, PASSIVE PROTECTION METHODS, STETHOSCOPE

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ……..…….....7
ВСТУП…….……...….8
1 ЗАГРОЗИ АКУСТИЧНІЙ ІНФОРМАЦІЇ…….……..….9
1.1. Шляхи втрати акустичної інформації…..…….…….....…9
1.2. Загрози акустичній інформації на об’єктах……..…...……..…12
1.3. Показник захищеності мовного повідомлення…….....25
2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ……..31
2.1. Методи забезпечення потрібної розбірливості мовного повідомлення…….31
2.2. Засоби прихованого отримання акустичної інформації.....37
2.3. Засоби забезпечення потрібної розбірливості мовного повідомлення……50
3. ТЕХНОЛОГІЯ ЕФЕКТИІНОГО ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ……..…….....57
ВИСНОВКИ……..…….…….……70
ПЕРЕЛІК ПОСИЛАНЬ…….…….....71

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ГШ	–	генератор шуму
ЗІ	–	захист інформації
ІзОД	–	інформація з обмеженим доступом
НСД	–	несанкціонований доступ
НЧ	–	Низькочастотні
ОІД	–	об’єкт інформаційної діяльності
ПЗ	–	пасивні засоби
УЗ	–	ультразвуковий
ЦТ	–	цілком таємно

ВСТУП

Актуальність дослідження. Останнім часом відбуваються якісні зміни у процесах управління на всіх рівнях, які зумовлені інтенсивним впровадженням новітніх інформаційних технологій. Швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило необхідність підвищення рівня інформаційної безпеки.

Одним із шляхів витоку інформації є акустичний канал.

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

Об’єкт дослідження – Процес захисту інформації.

Предмет дослідження – Захист акустичної інформації.

Мета роботи – Розробка технології ефективного захисту акустичної інформації на режимних об’єктах.

Наукові завдання:

- проаналізувати загрози акустичний інформації на ОІД;
- зробити огляд методи та засоби захисту акустичної інформації;
- підвищити ефективність захисту акустичної інформації на режимних об’єктах.

Методи дослідження – системний аналіз, чисельні методи.

Практичне значення одержаних результатів полягає у підвищити ефективність захисту акустичної інформації на режимних об’єктах.

Розділ 1.
ЗАГРОЗИ АКУСТИЧНІЙ ІНФОРМАЦІЇ

1.1. Шляхи втрати акустичної інформації

Акустичні канали витоку інформації у якості середовища поширення акустичних сигналів можуть використовувати повітря, воду інші тверді середовища. У якості перетворювачів акустичних сигналів в електричні використовуються високочутливі мікрофони або п’єзоелектричні прилади.

Отримання акустичної інформації з використанням мікрофонів може здійснюватися [1]:

- при використанні портативних пристроїв звукозапису таких як диктофони, встановлених в виділеному приміщенні для зняття конфіденційної акустичної інформації;

- з використанням новітніх електронних пристроїв перехоплення інформації (закладних пристроїв) з датчиком мікрофонного типу (перетворювачі акустичних сигналів, що поширюються в повітряному середовищі), скритно на об’єкті інформаційної діяльності, з передачею інформації по радіоканалу, оптичному каналу, електромережі 220 В, телефонної лінії, з'єднувальним лініях ДТЗС і спеціально прокладених кабелях;

- з використанням спрямованих мікрофонів, розміщених в оточуючих будівлях і транспортних засобах, які перебувають за межею контрольованої зони;

- без застосування технічних засобів (через недостатню звукоізоляцію огороджувальних конструкцій виділених приміщень і їх інженерно-технічних систем) сторонніми особами (відвідувачами, а також підкупним персоналом) при їх знаходженні в коридорах і прилеглих приміщеннях (ненавмисне прослуховування).

Застосуввання тих чи інших засобів акустичної розвідки на об’єкті інформаційної діяльності визначається можливістю доступу в контрольоване

приміщення сторонніх осіб. Недоліком способу перехоплення мовної інформації з використанням портативних диктофонів є необхідність повторного проникнення на об’єкт інформаційної діяльності з метою вилучення диктофона для прослуховування записаних розмов керівниками. Такого недоліку на сьогодні позбавлені електронні пристрої перехоплення інформації (закладні пристрої жучки). Під закладними пристроями зазвичай розуміють портативні пристрої знімання інформації, таємно закладаються в виділені приміщення, в тому числі в огороджувальні конструкції, обладнання, предмети інтер'єру, а також в технічні засоби і системи обробки інформації, в розетки, де вони можуть отримувати живлення, допоміжні технічні засоби і системи. Перехоплена інформація акустичними закладками може передаватися на приймальні пункти по радіо і оптичному каналі, спеціально прокладених лініях, електромережі змінного струму, телефонних лініях і т.д.

У тому випадку, якщо є постійний неконтрольований доступ відвідування під різними приводами (наприклад, для перевірки системи освітлення на об’єкті, кондиціонування або прибирання приміщення), то для перехоплення мовної інформації можуть використовуватися портативні пристрої звукозапису (в основному цифрові диктофони), які приховано встановлюються в інтер'єрах приміщень, як правило, безпосередньо перед проведенням закритого заходу. Після закінчення заходу диктофон з об’єкта інформаційної діяльності вилучається. Такі пристрої також можуть камуфлювати під предмети повсякденного побуту, наприклад, книги, письмові прилади, пачки сигарет і т.д. На теперішній час закордонними та вітчизняними фірмами випускається величезна кількість різних портативних цифрових диктофонів, які дуже легко заховати практично в будь-якому приміщенні. Цифрові диктофони можуть бути вбудовані в авторучку, наручний годинник і т.п. Недоліком способу перехоплення мовної інформації з використанням портативних диктофонів є необхідність повторного проникнення на об’єкт інформаційної діяльності з метою вилучення диктофона для прослуховування записаних розмов. Такого

недоліку позбавлені електронні пристрої перехоплення інформації (закладні пристрої).

Акустичні шляхи витоку інформації можна класифікувати таким чином [3]:

- повітряні шляхи - за рахунок поширення акустичних коливань у вільному повітряному просторі (переговори на відкритому просторі, якщо відкриті двері, вікна та вентиляційні канали);
- вібраційні - за рахунок впливу звукових коливань на всі елементи і конструкції будівлі, викликаючи вібраційні коливання (огороджувальні конструкції (стіна, стеля, підлога, вікна, двері, короба вентиляційних систем тощо), а також інженерні комунікації (труба водопостачання, опалення). Для перехоплення акустичної інформації в таких випадках використовують контактні мікрофони(стетоскопи);
- оптико-електронні (лазерні шляхи) - за рахунок приймання та демодуляції відбитих від вібруючих під дією акустичних сигналів поверхонь приміщень (шибки, дзеркала,вікна) випромінювання;
- акусто-електричні - за рахунок впливу звукових коливань на ДТЗС (за рахунок зміни параметрів (ємність, індуктивність, опір) під дією акустичного поля,створюваного джерелами мовних сигналів та виникнення електрорушійної сили, або до модуляції струмів, що протікають по цим елементам, за рахунок «мікрофонних ефектів», за рахунок використання «високочастотних електромагнітних нав'язувань»);
- параметричні - за рахунок впливу звукових коливань на ОТЗ і ДТЗС (за рахунок паразитної модуляції інформаційними сигналами випромінювань гетеродинів радіоприймальних і телевізійних пристроїв, які будуть перебувати у приміщеннях, де ведуться конфіденційні переговори та наради, за рахунок утворення вторинних радіохвиль, «при високочастотному опроміненні» приміщення, де встановлені закладні пристрої, які мають елементи, параметри яких можуть змінюватись під дією мовного сигналу);
- через закладні пристрої - канали витоку акустичної інформації,

канали витоку видової інформації.

1.2. Загрози акустичній інформації на об’єктах

Можливість витоку інформації залежить від багатьох чинників, основними з яких є [6]:

-можливість створення зловмисниками каналів витоку інформації;

- умови забезпечення розвідувального контакту в рамках того або іншого каналу витоку інформації.

За допомогою каналу витоку конфіденційної інформації, який є фізичним шляхом від джерела закритих відомостей до зловмисника (конкурента),може бути реалізований несанкціонований доступ до обмежених відомостей. Обов’язково необхідні певні енергетичні, просторові і часові умови,а також відповідні технічні засоби сприйняття та фіксації інформації для його створення.

Основними загрозами безпеки інформації під час проведення наради виступають:

- підслуховування і несанкціонований запис мовної інформації за допомогою закладних пристроїв, систем лазерного підслуховування, стетоскопів, диктофонів;

- реєстрація інформації на неконтрольованій території за допомогою радіомікрофонів учасниками, що виконують агентурне завдання;

- перехоплення електромагнітних випромінювань при роботі звукозаписувальних пристроїв і електроприладів.

Такі загрози безпеки інформації, як модифікація і знищення в даному випадку не актуальні.

Витік акустичної інформації є можливим через двері, вікна, стіни, підлогу, стелю, батареї центрального опалювання.

Джерелами небезпечних сигналів у вигляді радіохвиль або електричних сигналів можуть бути звукопідсилювальні і звукозаписувальні засоби та засоби охоронної сигналізації, різні побутові прилади, розміщені в кімнаті для нарад.

Наявність фахівців з іншої організації підвищує вірогідність виникнення додаткових каналів витоку інформації, тобто зловмисник може одержати інформацію про те, що відбувається на нараді шляхом найму кого-небудь з присутніх на нараді.

У акустичному каналі можна виділити наступні шляхи розповсюдження акустичної хвилі: повітряне середовище кімнати, несучі стіни, тонкі стіни між кімнатою для проведення наради і кабінетами директора, двері, вентиляційний канал.

Структурний звук може розповсюджуватися також через стіни, перегородки, віконні рами, дверні коробки, по трубопроводам і коробам вентиляції.

Загрозу безпеці мовної інформації може представляти безпосереднє підслуховування та підслуховування за допомогою технічних засобів.

При безпосередньому підслуховуванні зловмисником акустичні канали, що розповсюджуються по приміщенню, а також через вікна, двері, вентиляцію, приймаються слуховою системою зловмисника. В даному випадку можливі наступні варіанти підслуховування під час проведення наради:

- підслуховування через двері;
- підслуховування через вікно (у випадку, якщо воно нещільно закрите);
- підслуховування через вентиляційний отвір.

Окремо необхідно виділити варіант, коли зловмисник є учасником наради. У даній ситуації дуже складно знайти вирішення проблеми, оскільки у випадку не використання зловмисником спеціальної апаратури, не можливо звинуватити його в злочині. Отже, при складанні списку учасників наради співробітники, які його складають повинні більш ретельно перевіряти кожного учасника та його особисті якості.

При безпосередньому підслуховуванні зловмисником може також вестися реєстрація підслуханої інформації. Такий варіант може бути здійснений шляхом простого запису на паперовий носій при розташуванні зловмисника в сусідній кімнаті.

Здійснення підслуховування безпосередньо через вхідні двері є складнішим завданням, оскільки в робочий час в коридорі можуть знаходитися співробітники і охорона, і подібна поведінка, природно, приверне їх увагу, навіть в тому випадку, якщо зловмисником є співробітникомустанови.

При ситуації коли зловмисник є учасником наради, ведення яких-небудь записів неможливе, оскільки всі учасники бачать один одного, і, у разі обговорення конфіденційної інформації, учасники наперед попереджені про те, що робити які-небудь записи під час наради заборонено [3].

Також прослуховування можна проводити через вікна і двері. Прослуховування через двері є досить складною проблемою для зловмисника, оскільки під час проведення нарад двері не залишаються відкритими. Але подібну загрозу не слід виключати повністю, оскільки можливі наступні непередбачені обставини:

- двері не щільно прикриті, є щілини;

- під час наради учасники можуть виходити і входити у разі виникнення необхідності, отже, двері будуть короткочасно відкриватися і закриватися.

Стосовно підслуховування мовної інформації при відкритих вікнах, то воно можливе за допомогою напрямлених мікрофонів. Випускається декілька модифікацій направлених мікрофонів, які сприймають і підсилюють звуки, що йдуть тільки з одного напряму і послабляють всю решту звуків.

Для закритого запису в самому приміщенні для нарад можуть бути використані мініатюрні автоматичні магнітофони, що відрізняються від широко використовуваних малогабаритних магнітофонів меншою швидкістю стрічка протяжний механізм і можливістю автоматично включатися при появі звукових сигналів.

Складемо список найбільш вірогідних каналів витоку інформації з даного приміщення:

- ненавмисне прослуховування переговорів через вікно, двері, стіни, підлогу і стелю;

- прослуховування переговорів за допомогою спрямованих мікрофонів;

- запис переговорів за допомогою лазерної апаратури;

- запис переговорів за допомогою закладних пристроїв (закладок);

- витік акустичної інформації через опалювальну систему;

- огтримання інформативних наведень з телефонної лінії;

- витік мовної інформації за рахунок наведень на елементи, що володіють мікрофонним ефектом (охоронні сповіщувачі);

- персонал (при проведенні наради в контрольоване приміщення можливе таємне занесення звукозаписувальної апаратури);

- через вентиляційний отвір у суміжні приміщення.

Акустичні канали створюються:

- за рахунок поширення акустичних (механічних) коливань у вільному повітряному просторі (переговори на відкритому просторі, в приміщенні при відкритих вікнах, кватирках, дверях, виток через вентиляційні канали);

- за рахунок впливу звукових коливань на елементи і конструкції будівель, викликаючи їх вібрацію (стіни, стеля, підлога, вікна, двері, вентиляційна система, труби водопостачання, опалення, мережі кондиціонування).

Електромагнітні канали за своєю фізичною природою та експлуатаційними особливостями технічних засобів, які забезпечують виробничу діяльність, є найбільш небезпечними та досить поширеними каналами отримання інформації.

Такі канали створюються через наявність у технічних засобах, джерел небезпечних сигналів,які використовуються у виробництві.

Передусім, до таких джерел відносять перероблювачі, якими є прилади, що трансформують зміни однієї фізичної величини в зміни іншої. У термінах електроніки перероблювач визначається як прилад, що перетворює неелектричну величину в електронний сигнал, або навпаки. Певні знання механізму роботи перероблювачів дають змогу визначати можливі неконтрольовані прояви фізичних полів, які і створюють електромагнітні канали витоку (передання) інформації. Водночас, враховуючи ідентичність технічних і

конструктивних рішень, електронних схем технічних засобів обробки інформації та забезпечення виробничої діяльності підприємств і банків, усім їм потенційно властиві ті чи інші канали витоку (передання) інформації. Тому у будь-якому випадку використання технічних засобів обробки та передання інформації створює небезпеку її безконтрольного витоку.

Матеріально-речові канали отримання інформації створюються через вивчення наслідків виробничої діяльності (зіпсовані документи або їх фрагменти, чернетки різного роду поміток, записів, листів і т. д.), викрадення, несанкціоноване ознайомлення, копіювання, фотографування, відеозапис документів, креслень, планів, зразків технічних або програмних засобів.

Також поряд з неправомірним отриманням інформації існують інші загрози, які не передбачають отримання інформації, але, у свою чергу є не менш небезпечними. Серед основних їх видів є такі, як знищення і модифікація (зміна змісту) інформації. У цьому разі,використання інформації стає неможливим самими власниками, хоч вона і не потрапляє до конкурентів чи злочинців. Тому слід зазначити, що до факторів, які створюють умови витоку (передання) інформації, за дослідженнями спецслужб, відносять такі як: Балакучість співробітників підприємства, фірм, банків, установ; Відсутність на підприємстві, фірмі, в банку, державній установі системи заходів, спрямованих на захист інформації від її витоку; безконтрольне використання інформаційних систем; Наявність передумов для виникнення серед співробітників конфліктних ситуацій (тобто людські чинники).

На підставі викладеного можна зробити висновок, що отримання інформації спецслужбами, конкурентами та зловмисниками здебільшого здійснюється через технічні засоби, які використовуються на фірмах, підприємствах, у банках, та через їхніх співробітників. Тобто в основу інформаційної безпеки має бути покладено важливі заходи захисту інформації в засобах і мережах її передання та обробки. А також необхідне створення відповідної нормативної бази, яка б регулювала порядок доступу, зберігання та використання інформації фірми, банку, підприємства.

При обробці інформації в автоматизованих системах на об'єктах інформаційної діяльності можливий її витік по так званим побічним технічним каналам витоку.

Фізичні процеси, що відбуваються в пристроях обробки інформації на ОІД при їх функціонуванні, створюють у навколишньому просторі побічні електромагнітні, акустичні та інші випромінювання, які в будь-якому випадку пов'язані з обробкою інформації.

Подібні випромінювання можуть виявлятися на досить значних відстанях (до сотень метрів) а, отже, використовуються зловмисниками, які намагаються отримати доступ до таємниць. Тому, перш за все, заходи, що стосуються захисту інформації, яка циркулює в технічних засобах, спрямовані, на зниження рівнів таких випромінювань.

Побічні електромагнітні випромінювання виникають внаслідок непередбачуваного схемою або конструкцією даного технічного засобу передачі інформації по паразитних зв'язках напруги, струму, заряду або магнітного поля.

Під паразитним зв'язком - розуміють зв'язок по електричних або магнітних ланцюгах, що з'являється незалежно від бажання конструктора. Залежно від фізичної природи елементів паразитних електричних ланцюгів, розрізняють паразитний зв'язок через загальний повний опір, ємкісний або індуктивний [4].

Під технічним каналом витоку інформації розуміється сукупність фізичних полів несучих конфіденційну інформацію, конструктивних елементів взаємодіючих з ними, і технічних засобів зловмисника для реєстрації поля і зняття інформації. Перехоплення інформації за допомогою технічних засобів може здійснюватися тільки за межами контрольованої зони - території об'єкта, на якій виключено неконтрольоване перебування осіб і транспортних засобів, які не мають постійних або разових перепусток.

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

Такими засобами можуть бути:

- мережі електроживлення і лінії заземлення;
- автоматичні мережі телефонного зв'язку;
- системи телеграфного, телекодової та факсимільного зв'язку;
- засоби гучномовного зв'язку;
- засоби звуко- та відеозапису;
- системи звукопідсилення мови;
- електронно-обчислювальна техніка;
- електронні засоби оргтехніки.

Джерелом випромінювання в технічних каналах витоку інформації може бути і голосовий тракт людини, що викликає появу небезпечних акустичних випромінювань в приміщенні або поза ним. Якщо при цьому для перехоплення інформації використовується відповідна техніка, то утворюється технічний канал витоку інформації, званий акустичним.

Для її перехоплення передбачуваний «противник» може використовувати широкий арсенал портативних засобів акустичної мовної розвідки, які дозволяють перехоплювати мовну інформацію по прямому акустичному, віброакустичному, електроакустичному і оптико-електронному (акустооптичному) каналах, до основи яких ставиться :

• портативна апаратура звукозапису (малогабаритні диктофони, магнітофони та пристрої запису на основі цифрової схемотехніки);

• спрямовані мікрофони;

• електронні стетоскопи;

• електронні пристрої перехоплення мовної інформації (закладні пристрої) з датчиками мікрофонного і контактного типів з передачею перехопленої інформації по радіо, оптичному (в інфрачервоному діапазоні довжин хвиль) і ультразвуковому каналам, мережі електроживлення, телефонних лініях зв'язку, з'єднувальним лініях допоміжних технічних засобів або спеціально прокладених лініях;

- оптико-електронні (лазерні) акустичні системи й т.д.

У акустичних технічних каналах витоку інформації середовищем

поширення акустичних сигналів є повітря.

Звукові хвилі надають змінний тиск на предмети, розташовані на їх шляху, викликаючи механічні коливання в твердому тілі із звуковою частотою. В окремих конструкціях ці коливання можуть передаватися на значні відстані, майже не затухаючи, і знову випромінюватися в повітря, як чутний повітряний звук. Особливо добре випромінюють звук легкі будівельні конструкції з великою площею поверхні. Переданий звук носить назву «структурний звук».

Для перехоплення акустичної (мовної) інформації використовують такі пристрої:

- портативні диктофони і провідні мікрофонні системи прихованої звукозапису;

- спрямовані мікрофони;

- акустичні радіо-закладки (передача по радіоканалу);

- акустичні мережеві закладки (передача інформації з мережі живлення 220 В);

- акустичні інфрачервоні - закладки (передача інформації по оптичному каналу в інфрачервоному діапазоні довжин хвиль);

- акустичні телефонні закладки (передача інформації по телефонній лінії на високій частоті);

- акустичні телефонні закладки типу «телефонне вухо» (передача інформації по телефонній лінії на низькій частоті).

Найбільш поширеними засобами несанкціонованого отримання інформації, з якими фахівцям з ЗІ часто доводиться стикатися на практиці [4].

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

2. Гостронаправлені мікрофони, мають гостру діаграму спрямованості. За допомогою такого мікрофона можна прослухати розмову на відстані до 1 км в межах прямої видимості. За рухливим автомобілем аудіоконтроль вести можна тільки в тому випадку, якщо в ньому заздалегідь була встановлена закладка. На

тривалих зупинках бесіду можна прослуховувати спрямованим мікрофоном за умови, що автомобіль знаходиться в зоні прямої видимості і в ньому опущено одне із вікон . У громадських місцях (кафе, ресторан і т.п.) прослуховування можна здійснювати спрямованим мікрофоном або закладкою. У таких випадках гучна музика, як втім і шум води, що ллється, не рятують, так як у спрямованого мікрофона дуже вузька діаграма спрямованості.

3. Засоби прослуховування телефонних розмов можуть здійснювати несанкціоноване отримання інформації по телефонній лінії кількома методами:

- установка записуючої апаратури (ЗА) на АТС з використанням несумлінності або недбалості обслуговуючого персоналу;

- безпосереднє підключення ЗА до телефонної лінії (наприклад, в розподільній коробці);

- вбудовування схеми несанкціонованого підключення в телефонний апарат (для цього необхідний доступ в приміщення, в якому встановлений цей апарат).

Телефони, де в якості викличного пристрою використовується електромагнітний дзвінок можна прослуховувати через ланцюг дзвінка. Це можливо і в тому випадку, якщо трубка лежить на апараті через мікрофон [4]. Ще одним пристроєм прослуховування телефонних розмов і аудіо контролю приміщень може служити закладка, що живиться енергією самої лінії. Це пристрій зручний тим, що не вимагає заміни харчування - встановивши його одного разу, зловмисник може користуватися ним нескінченно довго. Працює вона тільки при знятій трубці. Якщо ж схема несанкціонованого підключення вбудована в телефон, то зловмиснику досить набрати номер цього телефону і пустити в лінію звуковий код, після чого заставна схема імітує відповідь на дзвінок і підключає телефон до лінії.

4. Якщо в приміщенні віконні скла не завішані, то розмову за такими вікнами можна прослухати, направивши на скло лазерний промінь. Звукові коливання в приміщенні призводять до синхронної вібрації стекол, а вони

модулюють лазерний промінь, який відображається від скла та надсилається на приймальний пристрій.

5. Приміщення, в яких не було проведено спеціальні заходи щодо ЗІ, можна прослуховувати за допомогою пристроїв, що реєструють коливання елементів конструкції будівлі (розетки, батареї центрального опалення, вентиляція, тонкі перегородки і т.п.).

6. Найбільш серйозну загрозу з точки зору ЗІ, можуть завдати зловмисники, які роблять спробу несанкціонованого доступу до інформації, яка обробляється автоматизованими системами (окремими комп'ютерами, інтелектуальними мережевими пристроями, локальними і розподіленими комп'ютерними мережами тощо).

Для отримання такої інформації можуть застосовуватися пристрої, що реєструють випромінювання комп'ютера і його периферії, а також комп'ютерних ліній передачі інформації. Зокрема, під час роботи автоматизованих систем до живильної електричної мережі наводяться сигнали, які після відповідної обробки відображають повністю або частково інформацію про роботу пам'яті і периферії. Для дистанційного зняття інформації за рахунок побічного випромінювання комп'ютера і його периферії застосовують високочутливі широкосмугові приймачі, що дозволяють виконувати подальшу цифрову обробку перехопленого сигналу. Ще одним методом несанкціонованого отримання інформації з автоматизованих систем є застосування методів несанкціонованого доступу до автоматизованої системи на локальному або мережевому рівні.

До групи прослуховуючих пристроїв відносяться: приймальна, передавальна апаратура, мікрофони, електронні стетоскопи, магнітофони та апаратура прослуховування телефонів, факсів, телексів.

Прослуховування - спосіб ведення розвідки, застосовуваний агентами, спостерігачами, спеціальними постами прослуховування. Це один з найпоширеніших способів отримання (добування) інформації.

Прослуховування може здійснюватися безпосереднім сприйняттям акустичних коливань при прямому сприйнятті мовної інформації, або сприйнятті

звукових коливань, що надходять через елементи будівель і приміщень (стіни, підлоги, стелі, вентиляційні канали, системи опалення), а також за допомогою досить різноманітних технічних засобів. До цього слід додати, що прослуховування ведеться в реальному масштабі часу і в певній мірі може дозволити своєчасно прийняти важливі оперативні рішення.

Прослуховування можна класифікувати наступним чином [4]:

1. Безпосереднє:

- пряме;

- через конструкції будівель і приміщень.

2. За допомогою технічних засобів:

- за допомогою мікрофонів;

- за допомогою радіо закладок;

- лазерне підслуховування.

Методика оцінки можливостей акустичної мовної розвідки по перехопленню мовної інформації за допомогою мікрофонів призначена для оцінки можливості перехоплення мовної інформації зі всіляких місць комунікативної діяльності людини (робочих і службових приміщень, кабінетів, відкритих просторів, квартир і т.п.) стаціонарною і портативною (з можливістю транспортування) апаратурою акустичної мовної розвідки з використанням різних типів мікрофонів [4].

З практичних міркувань може бути встановлена деяка шкала оцінок якості перехопленого мовного повідомлення:

- перехоплене мовне повідомлення містить кількість слів, що правильно розуміються, достатню для складання докладної довідки про зміст перехопленої розмови;

- перехоплене мовне повідомлення містить кількість слів, що правильно розуміються, достатню тільки для складання короткої довідки-анотації, що відображає предмет, проблему, мету і загальний сенс перехопленої розмови;

- перехоплене мовне повідомлення містить слова, що окремо правильно розуміються, достатню тільки для встановлення предмета розмови;

- при прослуховуванні фонограми перехопленого мовного повідомлення можливо встановити факт наявності мови, але не можна встановити предмет розмови.

Відповідно до ГОСТ Р 50840-95 розуміння переданої по каналах зв'язку мови з значною напруженістю уваги, перепитуваннями та повтореннями спостерігається при складовій розбірливості 25-40%, а при складовій розбірливості менше 25% мають місце нерозбірливості зв'язного тексту (зрив зв'язку) впродовж тривалих інтервалів часу. Враховуючи взаємозв'язок словесної і складової розбірливості, можна розрахувати, що зрив зв'язку спостерігатиметься при словесній розбірливості менше 71% [5].

Практичний досвід показує, що складання докладної довідки про зміст перехопленої розмови неможливий при словесній розбірливості менше 60-70%, а короткої довідки-анотації – при словесній розбірливості менше 40-50%. При словесній розбірливості менше 20-30% значно затруджене встановлення навіть предмету розмови, що ведеться, а при розбірливості менше 10%.

У зв'язку з вищевикладеним, як показник ефективності захисту акустичної інформації найчастіше використовують словесну розбірливість мови *W*.

Розрахунок словесної розбірливості мови приводиться для діапазону частот 250…5000 Гц, який відповідає п'яти стандартним октавним смугам частот з середньо геометричними частотами 250, 500, 1000, 2000, 4000 Гц.

Оцінку протидії акустичній мовній розвідці слід проводити при нормованому акустичному сигналі з інтегральним рівнем звукового тиску Lн, рівним 70 дБ.

В межах контрольованої зони для приміщення, що захищається, з метою виключення можливості ненавмисного прослуховування мови (без використання технічних засобів) особами, не допущеними до конфіденційної інформації,

необхідно відповідними технічними заходами забезпечити за межами огороджувальних конструкцій приміщень величину словесної розбірливості.

Методика оцінки можливостей акустичної мовної розвідки по перехопленню мовної інформації з використанням оптико-електронної (лазерної) апаратури.

Одним з головних каналів витоку інформації - телефонні та інші розмови, які при сучасному рівні розвитку техніки прослуховуються без особливих труднощів. Розмови можуть прослуховуватися як в приміщенні, так і в автомобілях. Пристрої аудіо-спостереження, за допомогою яких ведеться прослуховування, легко встановити і вкрай важко виявити, оскільки сучасна апаратура мініатюрна, надійна і має тривалий термін дії.

Для прослуховування широко використовуються різні прилади: радіомікрофони, спеціальні магнітофони, замасковані диктофони, стетоскопи і різні приймально-передавальні системи. Найпростіша і найбільш популярна система звукозапису складається з мікрофона, радіопередавача і джерела живлення. Деякі типи мікрофонів розраховані на збір інформації в радіусі 20 м і передачу її на відстань до 1 км Щоб виключити можливість виявлення, потужність передавача робиться невеликою. Цієї ж мети можна досягти шляхом правильного вибору робочої частоти. Широке поширення отримали перехоплюючі пристрої, що працюють в гігагерцевому діапазоні, що забезпечує велику проникність в бетонних будівлях.

1.3 Критерій розбірливості мовного повідомлення

Основною характеристикою будь-якого шляху передачі мовлення є зрозумілість мовлення. Для визначення цієї характеристики застосовується статистичний метод за участі великої кількості слухачів та дикторів. Розроблений непрямий метод визначення зрозумілості мовлення через його розбірливість. Під розбірливістю мовлення розуміють відносну або процентну кількість прийнятих (зрозумілих) елементів мовлення із загальної кількості елементів, переданих по каналу. Елементи мовлення складають склади, звуки, слова, фрази, цифри. У відповідність до них поставлені складова, звукова, словесна, смислова і цифрова розбірливості. Переважне застосування на практиці отримали складова, звукова і словесна розбірливість. Для оцінки розбірливості розроблені артикуляційні таблиці складів, звукосполучень і слів з урахуванням особливостей української мови.

Оцінка розбірливості проводиться за допомогою артикуляційної групи тренованих слухачів і дикторів без порушення слуху та мовлення. Такий метод називається артикуляційним [6].

Для визначення зв'язку між розбірливістю, виміряною артикулянтами, і зрозумілістю мови для звичайних людей були проведені масові випробування. Розмова велася за спеціальними розмовниками в обидві сторони, як при телефонних переговорах. При цьому контролювалося розуміння абонентами один одного. Оцінка зрозумілості ставилася за п'ятибальною системою. Одночасно для кожного з умов випробувань і кожного тракту були виміряні величини розбірливості мови за допомогою фахівців.

Одночасно із вказаними випробуваннями були виміряні статистичні залежності між складовою, словесною, звуковою і смисловою розбірливістю для української мови.

Формантна теорія, розроблена Флетчером і Коллардом, дозволила встановити безпосередній зв’язок між розбірливістю мовлення і характеристиками тракту передачі мовлення.

Звукові одиниці характеризуються різноманітними властивостями в залежності від різноманітних факторів їх розгляду. Утворенню звукових одиниць відповідає артикуляційний фактор, який називають анатомо-фізіологічним.

Акустичний фактор відноситься до властивостей звукових одиниць в результаті роботи вимовних органів і визначає звучання мови. Сприйняття звуків людиною відноситься до перцептивного фактору.

Таблиця 1.1.

Градації зрозумілості мовлення і відповідні їм розбірливості

Зрозумілість	Розбірливість, %	
	Складова	Словісна
Гранично допустима	25-40	75-87
Задовільна	40-50	87-93
Добра	50-80	93-98
Відмінна	80 і вище	98 і вище

Спочатку опис звукових систем здійснювався на основі аналізу артикуляції. Але з розвитком техніки акустичного аналізу звуків дослідники прийшли до висновку, що акустичні характеристики мови найбільш важливі. Сучасна фонетика враховує тісний зв'язок і взаємозумовленість між артикуляційними та акустичними характеристиками мови.

Звуки мови є складними звуками в основному через те, що процес мовоутворення супроводжується резонансними явищами, власні частоти яких змінюються в залежності від того, який звук в даний момент вимовляється.

Джерело звуку викликає в системі резонаторів мовотворчого тракту власні коливання. Звуки на власних частотах резонаторів є найбільш

посиленими. Власні частоти резонаторів називають формантами звуку, так як вони формують характерне звучання голосних і приголосних.

Частоти формант визначаються конфігурацією мовного тракту, і властивості джерела звуку на них не впливають. Це одне з найважливіших положень акустичної теорії мовоутворення. Це положення дозволяє пов'язувати частоти формант тільки зі специфікою артикуляції і по частотам формант судити про становище артикуляційних органів.

Число формант, які суттєво характеризують певний звук мови, дослідники визначають по різному, але в більшості випадків дослідники вважають, що в утворенні певного звуку беруть участь чотири форманти.

Форманти звуків мови заповнюють весь частотний діапазон від 150 до 7000 Гц. Середня ймовірність появи формант в тій чи іншій ділянці частотного діапазону для кожної мови цілком визначена. Погоджено ділити весь частотний діапазон на 20 смуг (в тому числі і для української мови) з однаковою ймовірністю появи формант в кожній з них. Відповідні смуги називаються смугами рівної розбірливості. Виявлено, що при досить великому обсязі переданої мови ймовірності появи формант відповідають правилу адитивності. Внаслідок цього ймовірність появи формант в кожній смузі рівній розбірливості дорівнює 0,05.

Якщо сприймати мову в умовах шумів і завад, то її розбірливість виходить меншою. Це пов'язано з тим, що форманти мають різні рівні інтенсивності: у гучних звуків вище, ніж у глухих. Тому, при підвищенні рівня шумів спочатку маскуються форманти з низькими рівнями, а потім з більш високими. При збільшенні рівня шумів і завад ймовірність сприйняття формант поступово зменшується. Коефіцієнт, що визначає це зменшення, називають коефіцієнтом сприйняття або коефіцієнтом розбірливості w. У кожній смузі ймовірність прийому формант буде $\Delta A = 0{,}05w$.

Через те, що вся енергія звуків мови в основному зосереджена в формантах, то рівні формант практично збігаються з рівнями звуків мови. Поріг чутності в шумах визначається спектральними рівнями шумів. Різниця між

середнім спектральним рівнем мовлення і спектральним рівнем шумів буде визначати ймовірність появи формант вище рівня шумів [8].

Коефіцієнт розбірливості w визначається рівнем відчуття формант:

$$E = B_p - B_ш$$

де:

$B_р$ – середній спектральний рівень мовлення;

$B_ш$ – спектральний рівень шумів.

Для рівнів відчуття, що знаходяться у межах 0-18 дБ, коефіцієнт розбірливості можна визначити за наближеною формулою $w = (E + 6)/30$.

Для кожної смуги рівної розбірливості коефіцієнт розбірливості (w_n) буде різним. Тоді сумарна ймовірність прийому формант (розбірливість формант) визначається як:

$$A_ф = \sum_{n=1}^{20} 0,05 w_n$$

В закритих приміщеннях звукові хвилі багаторазово відбиваються від захисних поверхонь, в результаті чого створюється складна картина звукового поля. Закони розподілу характеристик звукового поля в даній ситуації визначаються не тільки властивостями джерела звуку, але і іншими факторами – геометрією приміщення, здатністю стін, стелі і підлоги поглинати та відбивати звукову енергію. Тому звукові поля в закритому приміщенні і у вільному просторі мають різні структури. Якщо у вільному просторі інтенсивність звуку визначається потоком енергії у напрямку поширення хвилі, то в приміщенні результуючий потік енергії має дві складові – прямий потік та відбитий (іноді багаторазово) потік. Направлення потоків енергії відбитих хвиль залежить від особливостей планування приміщення та ступеня поглинання звукової енергії поверхнями захисних конструкцій. В цій ситуації визначення інтенсивності звуку в класичному розумінні неприйнятно.

Прийнятною енергетичною характеристикою звукового поля в приміщенні є густина звукової енергії ε.Якщо приміщення не має фокусуючих поверхонь і геометрично симетричних перерізів, а розміри приміщення значно більші довжини хвилі і якщо захисні конструкції не сильно поглинають звукову енергію, то через деякий час за неперервної дії джерела звуку через вільний елемент перерізу приміщення в кожний момент часу буде проходити більше число окремих хвиль, що поширюються за різними напрямками. В результаті звукове поле буде характеризуватися наступними властивостями:

- потоки енергії цих хвиль за всіма напрямками рівноймовірні;
- густина звукової енергії ε звукового поля по всьому об'єму приміщення постійна.

Рівноймовірність потоків енергії хвиль називають ізотропією звукового поля, а сталість звукової енергії по всьому об'єму приміщення – однорідністю. Якщо звукове поле є ізотропним і однорідним, то його називають дифузним. Для дифузного поля характерна відсутність явищ інтерференції.

Процес нарощування густини звукової енергії в приміщенні протікає дуже швидко і непомітно для слуху. Процес спаду (поглинання) звукової енергії, що називається реверберацією, проходить повільніше і помітно для слуху. Реверберація впливає на слухове сприйняття.

Поглинання звукової енергії здійснюється не тільки захисними конструкціями приміщення, але і повітряним середовищем. Втрати енергії в повітряному середовищі обумовлені в'язкістю та теплопровідністю повітря, а також молекулярним поглинанням. Поглинання звукової енергії повітрям залежить від пробігу звукової хвилі і визначається як:

$$\varepsilon = \varepsilon_0 e^{-\mu l}$$

де:

$l = c_{зв} t$ – довжина пробігу звукової хвилі;

ε_0 – усталена густина звукової енергії в приміщенні; μ – коефіцієнт затухання; рівний зворотному значенню шляху, на якому густина енергії зменшується в e разів.

Коефіцієнт затухання $\mu = 52{,}5\frac{F^2}{c\rho_0}\eta$залежить від густини ρ_0, в'язкості η повітря, частоти F, а також від температури та вологості повітря.

Висновок по розділу.

Акустична інформація втрачається повітрянимми шляхами, вібраційними, оптико-електронними (лазерні шляхи), акусто-електричними, параметричними, через закладні пристрої.

Перетворення акустичних сигналів в електричні здійснюється застосуванням мікрофонів та п’єзоелектричних приладів.

Критерієм оцінки захищеності акустичної інформації є словісна розбірливість мови.

Розділ 2.
МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ

2.1 Методи забезпечення потрібної розбірливості мовного повідомлення

Методи захисту інформації від витоку повітряним, віброакустичним та оптоелектронним каналами зводяться до зниження рівня акустичних/віброакустичних сигналів (озвучення інформації) до певного співвідношення сигнал/завада, що визначається потрібною розбірливістю мовного повідомлення.

Потрібного співвідношення сигнал/завада, а отже і розбірливості мовного повідомлення можна досягнути пасивними або активними методами.

Пасивні методи захисту інформації спрямовані на підвищення звукоізоляції огороджувальних конструкції ОІД (встановлення металопластикових вікон, ущільнювачів дверей, створення «плаваючої підлоги», встановлення акустичних фільтрів у повітроводи тощо) [4].

Активні методи захисту інформації спрямовані на зниження співвідношення сигнал/завада до норми шляхом створення акустичної\віброакустичної завади на межі огороджувальних конструкцій ОІД [9] (рис. 2.1.).

Рис. 2.1 Методи захисту акустичної інформації

Організаційні заходи.

Нарада за участю представників сторонніх організацій має проводитися з дозволу керівника, який, у свою чергу, призначає відповідального за проведення наради.

Відповідальна особа, спільно з представниками служби безпеки та відповідними технічними фахівцями проводить необхідні організаційні та технічні заходи, спрямовані на забезпечення збереження секретності обговорюваних питань.

Черговість розгляду питань, винесених на нараду, повинна виключати участь осіб, які не мають відношення до питань, які розглядаються. Відповідальна особа має скласти проект програми наради та список учасників, в якому вказується прізвище, ім'я по батькові, місце роботи, посаду і питання, в обговоренні яких він може приймати участь. Учасники пропускаються на нараду за списками при пред'явленні документів, що засвідчують особу.

Доцільно і обґрунтовано застосування наступних організаційних заходів:

- перед проведенням наради необхідно проводити візуальний огляд приміщення на предмет виявлення закладних пристроїв. Огляд повинен проводитися систематизовано і ретельно, звертаючи увагу на будь-яку дрібницю, на перший погляд незначну: наявність сторонніх предметів, побутової апаратури або предметів інтер'єру. Огляд по можливості, повинен проводитися співробітником служби безпеки і людиною, добре знайомим зі звичайною обстановкою залу, наприклад, співробітником охорони;

- безпосередньо перед проведенням наради охорона повинна оглядати прилеглі до кімнати для нарад приміщення, на предмет видалення з них співробітників або сторонніх осіб, які можуть вести підслуховування безпосередньо через систему вентиляційних комунікацій або через стіну за допомогою спеціальної апаратури; закривати ці приміщення на час проведення наради і вести контроль за доступом у них;

- кількість осіб, які беруть участь у конфіденційних переговорах має

бути обмежена до мінімуму;

- вхід сторонніх осіб під час проведення наради має бути заборонений;

- повинна бути чітко розроблена охорона виділеного приміщення підчас наради, а також спостереження за обстановкою на поверсі. Під час проведення закритої наради необхідно не допускати близько до дверей кімнати нікого зі сторонніх осіб або співробітників організації. Стоячи під дверима, або поблизу від неї, зловмисник може підслухати те, про що говориться в кімнаті. Особливо це ймовірно в ті моменти, коли хтось входить або виходить із залу, тому що на той час, поки двері залишаються відкритими, розбірливість мовлення різко підвищується. Крім цього, виходячи або входячи, людина може не зовсім щільно закрити за собою двері, що також підвищить розбірливість мовлення. Для реалізації цього заходу необхідно, щоб протягом всього часу, яке триває нарада, біля дверей кімнати чергував охоронець, який здійснює контроль за дверима і коридором біля входу в кімнату, а також стежити за тим, щоб ніхто зі сторонніх не проник всередину.

По можливості проведення нарад переносити на неробочий час.

Будь-які роботи в кімнаті, що проводяться поза часом проведення конфіденційних нарад, наприклад: прибирання, ремонт побутової техніки, дрібний косметичний ремонт, повинен проводитися в обов'язковій присутності співробітника служби безпеки. Наявність цих співробітників допоможе убезпечити приміщення від установки підслуховуючих пристроїв співробітниками організації або ж сторонніми особами (електромонтер, робочі, прибиральниця і так далі).

Після проведення наради кімната повинна ретельно оглядатися, закриватися і опечатуватися.

Між нарадами кімната повинна бути закрита, і опечатана відповідальною особою. Ключі від кімнати повинні бути передані черговій зміні охорони під розписку і зберігатися в кімнаті охорони, доступ до них повинен бути регламентований керівництвом.

Перелічені заходи організаційного захисту інформації в кімнаті для нарад вважаються вельми дієвими і не несуть серйозних матеріальних витрат або проблем з персоналом та можуть застосовуватися як окремо, так і разом, що дозволить значно підвищити ступінь захисту інформації розглянутого об'єкта.

Заходи протидії отриманню акустичної інформації через закладні пристрої.

Автономні пристрої, які конструктивно об'єднують мікрофони і передавачі, називають закладними пристроями перехоплення мовної інформації.

Перехоплена ЗП мовна інформація може передаватися по радіоканалу, мережі електроживлення, оптичному каналу, з'єднувальним лініям ДТЗС, стороннім провідникам, інженерним комунікаціям в ультразвуковом діапазоні частот, телефонної лінії з викликом від зовнішнього телефонного абонента.

Прийом інформації, що передається ЗП, здійснюється, як правило, на спеціальні приймальні пристрої, які працюють у відповідному діапазоні довжин хвиль. Однак існують винятки з цього правила. Так, у випадку передачі інформації по телефонній лінії з викликом від зовнішнього абонента прийом можна здійснювати зі звичайного телефонного апарату.

Використання портативних диктофонів і ЗП, як правило, вимагає проникнення в контрольоване приміщення. Але, у деяких випадках проникати до приміщення не обов’язково, наприклад при застосування стетоскопів.

Використання ЗП вимагає проникнення до контрольованого приміщення (контрольовану зону). Коли це не вдається, для перехоплення мовної інформації використовуються спрямовані мікрофони.

Виявлення ЗП являє собою специфічний вид робіт тому він виділяється в окрему категорію робіт з технічного захисту інформації.

Насамперед, необхідно вжити заходів для підвищення звукоізоляції приміщення ОІД. До них можна віднести таки вимоги [10]:

1. Приміщення, де планується створення ОІД, повинне мати подвійні вхідні двері, що мають щільну підгонку до дверної коробки, між якими утворюється тамбур, якій має по периметру дверей ущільнюватися гумовими прокладками.

Поверхні тамбура облаштовуються звукопоглинаючими матеріалами, на підлозі встановлюються пороги. Чим більше глибина тамбура, тим вище звукоізоляція. При наявності додаткового (запасного) виходу з об’єкта, якщо він не проходить через повністю контрольовані приміщення, куди не можуть потрапити сторонні особи (наприклад, вихід здійснюється через кімнату відпочинку, підсобні приміщення тобто «зону неможливого прослуховування»), конструкція дверей повинна бути такою самою як і основних дверей.

2. Стіни та перегородки об’єкту повинні бути бетонними (залізобетонними) завтовшки не менше ніж 80 мм або цегляними завтовшки не менше ніж 120 мм, оздоблені звукопоглинаючими декоративними матеріалами.

Високу звукоізоляцію дають стіни, які мають багатошарову конструкцію з використанням звукопоглинаючих матеріалів (наприклад, гіпсокартон - мінеральна вата - цегла). При цьому, така конструкція не повинна містити металевих елементів (профілів для кріплення гіпсокартону, сітки-рабиці тощо).

Стіни повинні надійно з’єднуватися з верхнім та нижнім міжповерховим перекриттям. Об’єкт не може мати спільній простір під підвісною стелею або підлогою з іншими приміщеннями.

3. Міжповерхові перекриття не повинні містити будь-яких отворів (штучних або природних) з боку об'єкта. Якщо вони вже є, їх слід заповнити на всю глибину будівельною сумішшю (наприклад, цементно-піщаною).

4. Стеля крім декоративної функції повинна підвищувати звукоізоляцію об’єкта. Як варіант – підвісна, на еластичних підвісах, яка складається з окремих звукопоглинаючих плит. При цьому, вона не повинна мати закритих порожнин, доступ до яких ускладнений. Увесь простір під і над підвісною стелею повинен легко оглядатися.

5. Підлогу бажано зробити багатошарову (наприклад, на основі паркету, паркетної дошки, ламінованого покриття тощо) із звукопоглинаючим матеріалом усередині, яка побудована за принципом „плаваючої підлоги”.

Плінтус по периметру приміщення бажано застосовувати з еластичними краями та спеціальними каналами для кабельних комунікацій.

6. Вікна у приміщенні об’єкта бажано використовувати з підвищеною звукоізоляцією. Наприклад, металопластикові або дерев’яні з склопакетами, які мають не менше ніж дві камери (три скла).

Фурнітура повинна забезпечувати щільне прилягання до рами рухомих елементів вікна на протязі не менше двох років.

Після завершення будівництва (реконструкції, ремонту) на вікнах об’єкту необхідно встановити пристрої, які не дозволяють оглядати приміщення ззовні (штори, жалюзі тощо) незалежно від поверху і наявності будівель, розташованих навпроти.

Заходи спрямовані на протидію несанкціонованому доступу до приміщення або до окремих його елементів:

1. Вхідні двері зали для проведення секретних нарад з коридору обладнуються надійним замком, а також пристроєм, що сигналізує про доступ до об'єкту (чашка для опечатування, лічильник відкривання дверей, петлі для опломбування або використання плашок для опечатування тощо).

2. Кришки оглядових люків, інші елементи доступу до ніш, шахт тощо, в яких прокладені комунікації, обладнуються засобами замикання та пристроями для опломбовування.

3. Об’єкт оснащується охоронною сигналізацією, яка повинна бути виведена на пульт централізованого спостереження підрозділу охорони. Для живлення охоронної сигналізації в аварійних випадках має передбачатися автономне джерело живлення. Переключення на автономне джерело живлення має бути автоматичним.

Таким чином для запобігання витоку інформації пропонується комплекс організаційних і технічних заходів перед проведенням наради і в ході наради [11].

Основні організаційні заходи:

- перевірка приміщення перед проведення наради, з метою оцінки стану забезпечення безпеки інформації;
- управління допуском учасників наради до приміщення;

- організація спостереження за входом у обране приміщення і навколишнім оточенням в ході проведення наради.

Основними засобами забезпечення захисту акустичної інформації при проведенні наради є [11]:

- установка різних генераторів шуму, моніторинг приміщення на предмет наявності закладних пристроїв, звукоізоляція.

Основні технічні заходи захисту інформації:

- 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.

2.2. Засоби прихованого отримання акустичної інформації

Для перехоплення акустичної інформації використовуються наступні методи:

– пасивні методи перехоплення;
– активні методи перехоплення;
– контактні методи перехоплення.

За способом застосування технічні засоби отримання акустичної інформації можна класифікувати, наступним чином (рис. 2.2).

Засоби, що встановлюються заходовими (вимагають фізичного проникнення на об’єкт) методами [6]:

– радіозакладки;
– закладки з передачею акустичної інформації в інфрачервоному діапазоні;
– закладки з передачею інформації за допомогою мережі 220 В;
– закладки з передачею акустичної інформації за допомогою телефонної лінії;

– диктофони;

– провідні мікрофони.

Рис. 2.2 Класифікація засобів несанкціонованого зняття інформації

Засоби, що встановлюються беззаходовими методами (тобто не треба фізично проникати на об’єкт):

– апаратура, що використовує мікрофонний ефект;

– метод ВЧ нав’язування;

– електронний стетоскоп;

– лазерний стетоскоп;

– спрямований мікрофон.

Найбільш перспективним напрямком є використання лазерних мікрофонів, перші зразки яких були прийняті на озброєння американськими спецслужбами ще в 60-і роки.

Цей лазерний мікрофон був спеціально розроблений для урядових і правоохоронних організацій для прихованого використання в ситуаціях, коли вхід в будівлі не підходить або не підходить для розміщення прослуховувального пристрою в цільовій зоні. Пристрої лазерного прослуховування дальньої дії також не піддається виявленню, оскільки інфрачервоний лазер повністю невидимий для неозброєного ока.

На сьогоднішній день створено ціле сімейство лазерних засобів акустичної розвідки (рис.2.3).

Рис. 2.3 Лазерний засіб акустичної розвідки

Дана модель складається з джерела випромінювання (гелій-неоновий лазер), приймача цього випромінювання з блоком фільтрації шумів, двох пар головних телефонів, акумулятора живлення і штатива. Наведення лазерного випромінювання на шибку потрібного приміщення здійснюється за допомогою телескопічного візира. Змінювати кут розходження пучка дозволяє оптична насадка, висока стабільність параметрів досягається завдяки використанню

системи автоматичного регулювання. Забезпечується отримання мовної інформації з віконних рам з подвійними скельцями з гарною якістю на відстані до 500 м [12].

Досягнення в розвитку лазерної техніки дозволили значно поліпшити технічні характеристики і надійність роботи даних систем розвідки. Розглянемо більш докладно фізичні процеси, що відбуваються під час перехоплення мови за допомогою ЛСАР (рис.2.4).

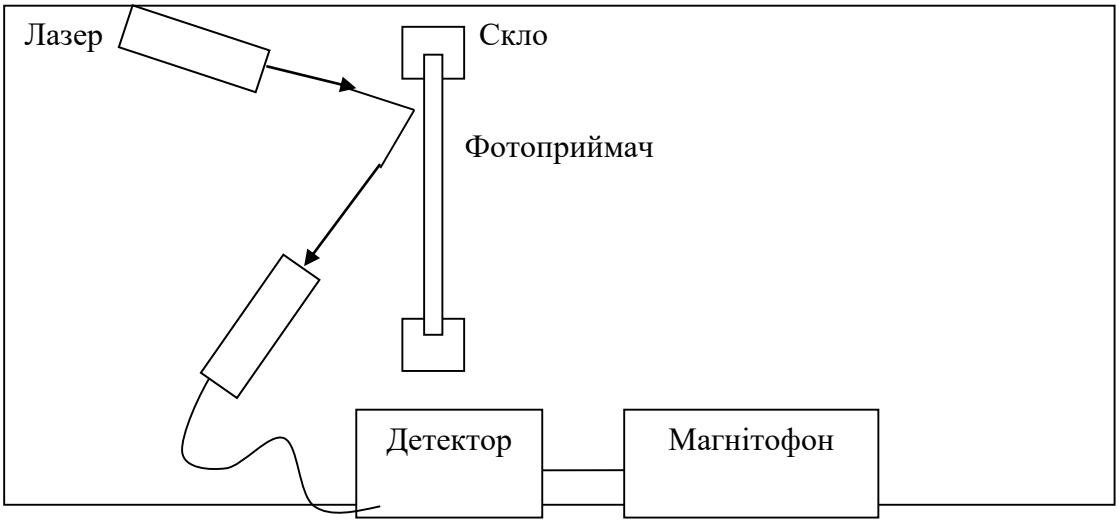


Рис. 2.4 Метод отримання інформації зі скла

Зондувальний об'єкт - зазвичай віконне скло - являє собою своєрідну мембрану, яка коливається зі звуковою частотою, створюючи фонограму розмови. Генерується лазерним передавачем випромінювання, поширюючись в атмосфері, відбивається від поверхні віконного скла і модулюється акустичним сигналом, а потім сприймається фотоприймачем, який і відновлює розвідувальний сигнал.

У даній технології принципове значення має процес модуляції, який можна описати таким чином.

Звукова хвиля, що генерується джерелом акустичного сигналу, падає на межу поділу повітря-скло і створює свого роду вібрацію, тобто відхилення поверхні скла від початкового положення. Ці відхилення викликають дифракцію

світла, що відбивається від кордону. Якщо розміри падаючого оптичного пучка малі в порівнянні з довжиною «поверхневої» хвилі, то в суперпозиції різних компонентів відбитого світла буде домінувати дифракційний пучок нульового порядку. У цьому випадку, по-перше, фаза світлової хвилі виявляється промодельованою за часом з частотою звуку і однорідною по перетину пучка, а по-друге, пучок «хитається» з частотою звуку навколо напрямку дзеркального відображення.

Необхідно враховувати, що на якість прийнятої інформації впливають такі чинники:

- параметри використовуваного лазера (довжина хвилі, потужність, когерентність) ;
- параметри фотоприймача (чутливість і вибірковість фотодетектора, вид обробки сигналу);
- параметри атмосфери (розсіювання, поглинання, турбулентність, рівень фонової засвітки);
- якість обробки зондувальної поверхні (шорсткості і нерівності, зумовлені як технологічними причинами, так і впливом середовища - бруд, подряпини та ін.);
- рівень фонових акустичних шумів,рівень перехопленого мовного сигналу;
- конкретні місцеві умови.

Всі ці обставини накладають свій відбиток на якість фіксування мови, тому не можна приймати на віру дані про прийом з дальності в сотні метрів - ці цифри отримані в умовах полігону, а то і розрахунковим шляхом.

Також існують стетоскопи для прослуховування через стіни та інші інженерні конструкції (рис.2.5).

Рис. 2.5 Електронний стетоскоп

Модель призначена для аудіо контролю приміщення в складних умовах. Мікрофон є «родичем» стетоскопа, тобто вузько направленим підсилювачем звуку. Мікрофон, має 2 насадки для зняття звуку через поверхню товщинною до 30 см

Перша насадка використовується в якості посилення звуку через стіну за принципом прикладання до поверхні. У центрі насадки виступає голка на 3 мм від площини і як тільки датчик звуку притискається до стіни і голка порівнюється з поверхнею, тут же звукові коливання по стіні посилюються багаторазово і передаються на блок мікрофона через стіну. Таким чином, ви можете чути, що відбувається за недоступною вам перешкодою.

Друга насадка на мікрофон призначена для тонких отворів 2 мм, і вона працює за принципом направленого мікрофона. Встановивши дуже тонку насадку в отвір, можна чітко почути, що відбувається в приміщенні. Всі деталі спрямованого мікрофона виконані зі сталі [13].

Професійний комплект для ведення прослуховування через стіни і склоF-999B дозволить Вам прослуховувати приміщення через бетонні, сталеві, металеві, дерев'яні та цегляні стіни, а також прослуховувати приміщення через скло і повітряні прошарки. У комплекті находиться високочутливий контактний

датчик жучок для прослуховування, який до поверхні кріпити не обов'язково, досить прикласти зонд для прослуховування через отвори і щілини. Можна прослуховувати розмову через навушники і приєднавши антену передавати звук по радіоканалу на частоті 100 МГц навіть на звичайний радіоприймач. Одночасно з цим є лінійний аудіо вихід, що дозволить вести запис розмови з прослуховувального пристрою на диктофон, ПК, ноутбук. Передбачене частотне регулювання звуку для отримання більш чистого результату. Живлення - вбудований акумулятор, час автономної роботи 100 годин.

Знімання інформації в теперішній час з використанням радіо закладних пристроїв (рис.2.6) є одним з найбільш поширених способів негласного отримання інформації. Радіозакладка – мініатюрний електронний пристрій, що складається з мікрофона і радіопередавача, що забезпечує передачу підслуховуваних переговорів на досить значну відстань за допомогою електромагнітних хвиль.

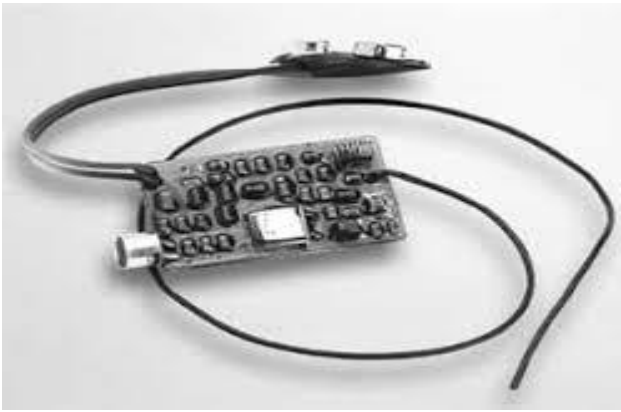


Рис. 2.6 Радіозакладний пристрій

Мікрофони, використовувані в радіо закладках, можуть бути двох типів:

- мікрофони що вловлюють акустичні коливання, які поширюються в повітряному просторі, наприклад в просторі службових приміщень. Радіозакладки, в яких використовуються подібні мікрофони, дозволяють вловлювати тиху мову на дальності 5 -10 метрів;

- мікрофони (контактні), що перехоплюють акустичні коливання по вібраційних каналах, тобто коливання, що поширюються в твердих конструкціях. Це можуть бути стіни, підлога, стеля, труби опалення, водопостачання, каналізації. Радіозакладки, в яких використовуються мікрофони даного типу, називаються радіо стетоскопами. Природа виникнення коливань в твердо тільних конструкціях є такою: звукова хвиля, переходячи з повітряної (простору приміщення) в тверду середу (стіну, стелю, підлогу), викликає в останньої коливання. Радіозакладки з мікрофонами такого типу (радіо стетоскопи) здатні вловлювати звукові коливання через бетонні стіни товщиною 0,3-0,5 м, а також через двері та віконні рами.

Передавач передає радіосигнали інформації за допомогою електромагнітних хвиль (в даному випадку в радіодіапазоні). Природно, для прийому інформації, яка передається радіозакладками необхідний приймач. Причому принципової відмінності подібного приймача від радіоприймача, встановленого в плеєрі, магнітоли, музичному центрі, немає. Все залежить від частоти, на якій працює радіозакладка. Теоретично, якщо у зловмисника немає необхідних для покупки спеціального приймача коштів, він може використовувати радіозакладки з частотою передачі в діапазоні, виділеному для радіомовлення, а в якості так званого розвідувального приймача використовувати радіоприймач, який продається в магазині побутової електроніки. Звичайно, вірогідність цього украй мала, адже тоді сигнал, який передається зможуть приймати всі власники радіоприймачів, що знаходяться в радіусі її дії. А це, самі розумієте, не тільки демаскує діяльність зловмисника, а й значною мірою сприяє його виявленнюта затримання служителями закону.

Також існують методи високочастотного нав’язування .

Для прослуховування телефонів широко використовуються такі способи, як підключення до телефонних ліній, установка в телефонну лінію телефонних радіозакладок, високочастотне нав'язування і інші варіанти підслуховування. Найбільшого поширення отримує установка телефонних радіозакладок.

У просторовому плані телефонна радіозакладка може бути встановлена в приміщенні, де зловмисникові потрібно контролювати телефонні переговори. Для цього телефонна радіозакладка може бути встановлена безпосередньо в телефонному апараті, розетці або підключена в будь-якій точці приміщення до телефонних дротів. За межами приміщення телефонна радіозакладка може бути встановлена в розподільній коробці і розподільній шафі будівлі. Всередині будівлі особливо вразливий тракт від телефонного апарату до розподільної шафи. В цьому випадку можлива як установка радіозакладок, так і підключення до лінії контактним або безконтактним способом.

Від розподільної шафи до АТС покладено багатожильний кабель, підключення до якого вельми скрутно.

Ще однією «слабкою» ланкою є АТС. На ній можливе підключення і установка радіозакладки безпосередньо до того чи іншого осередку.

Мікропередавач з контактним підключенням (діапазон 400-500 МГц, дальність 200 м) може встановлюватися на лініях від розподільної шафи АТС до розподільної коробки, від коробки до телефонної розетки(рис.2.5). Мікропередавач у вигляді конденсатора (діапазон 139 МГц, дальність 500-800 м) - на АТС, в розподільній шафі, в розподільній коробці, в розетку, в телефонному апараті. І нарешті в самому телефонному апараті може також встановлюватися мікропередавач у вигляді мікрофонного капсуля (діапазон 107-115 МГц, дальність до 100 м).

Прилад прослуховування телефону GSM жучок дозволяє вести акустичний контроль приміщення його підкладають в середину wi-fi роутератам. Він бере живлення і може на любій відстані по VPN вести коли потрібно отримання інформації (рис. 2.7).

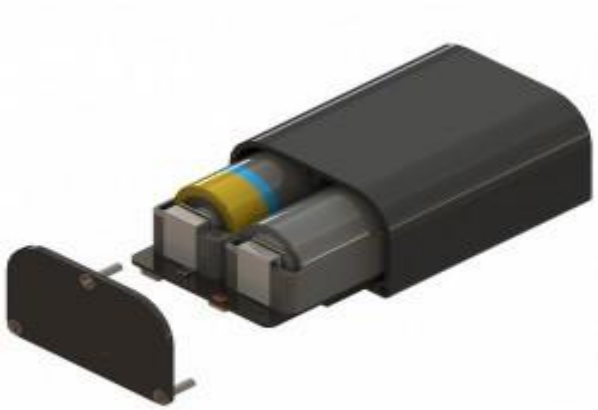


Рис. 2.7 GSM закладка

Пристрій передає сигнал по радіоканалу без обмеження відстані зловмиснику не потрібно навіть знаходитись в межах країни. Пристрій підключається паралельно до роутера, і живиться від нього, що вигідно відрізняє GSM жучок від інших приладів подібного класу, так як час роботи необмежено живленням. При покладеній трубці працює, як радіомікрофон з високою чутливістю, що дозволяє прослуховувати приміщення площею до 50 м^2, при піднятій трубці телефону пристрій переходить в режим телефонного радіопередавача, тобто прослуховується телефонна розмова. Також GSM жучок можливо змонтувати в інтернет кабель провайдера тільки тоді йому буде потрібно окремо подавати живлення 12 v , монтується крокодилами . Йому не потрібен пароль в нього вже прошитий VPN через котрий без всяких налаштувань і паролів здійснюється підключення до інтернету.

Спрямовані 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...70 м).

Основні характеристики спрямованих мікрофонів: тип мікрофона, дальність перехоплення, розміри частотний діапазон, коефіцієнт посилення, діаграма спрямованості

Найбільш відомі як найменш чотири види спрямованих мікрофонів [13].:

- параболічні;
- плоскі акустичні фазовані решітки;
- градієнтні;
- трубчасті, чи мікрофони "хвилі, що біжать".

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. 2.8 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 вибірковість за прийомом. Параболічний мікрофон є типовим прикладом високочутливого, але слабко направленого мікрофону. Прикладом є направлений мікрофон "Велике вухо", що випустили в ФРН.

Трубчасті мікрофони, чи мікрофони "хвиля, що біжить", на відміну від параболічних мікрофонів приймають звук не на площині, а вздовж деякої лінії, співпадаючої з напрямом на джерело звуку (рис. 2.9).

Рис.2.8 Параболічний мікрофон

Рис. 2.9 Трубчастий спрямований мікрофон

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 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.

2.3 Засоби забезпечення потрібної розбірливості мовного повідомлення

Призначенням (принцип дії) активних засобів захисту мовної інформації є:

- створення маскувальних акустичних і вібраційних шумів з метою зменшення відносин сигнал/шум до величин, що забезпечують неможливість виділення засобом акустичної розвідки мовної інформації в місцях їх можливого встановлення;

- створення маскувальних електромагнітних перешкод в сполучних лініях ДТЗС з метою зменшення відносин сигнал/шум до величин, що забезпечують неможливість виділення інформаційного сигналу засобом розвідки в можливих місцях їх підключення [14]..

Пристрій захисту від витоку акустичної інформації віброакустичний генератор білого шуму«DNG-2300» (рис. 2.10).

DNG-2300 є незамінним доповненням до комплексу найсучасніших засобів протидії інформаційному шпигунству, а також може застосовуватися самостійно з метою забезпечення периметру та захисту від витоку мовної інформації.

Шумова перешкода, що генерується DNG-2300 сформовано спеціальним чином з метою оптимального маскування сигналів мовного діапазону частот.

Віброакустичний генератор білого шуму DNG-2300 розроблений фахівцями фірми REI для нейтралізації підслуховуючих пристроїв, виявлення яких ускладнено традиційними засобами виявлення.

Прилад DNG-2300 забезпечує протидію таким видам підслуховуючих пристроїв як провідні мікрофони, вмонтовані в огороджувальні конструкції, контактні або проколюють мікрофони, радіопередавачі, встановлені в електричні розетки, а також лазерні та мікрохвильові системи знімання інформації з вікон будівельних конструкцій [15].

Рис. 2.10 Генератор білого шуму DNG-2300

Віброперетворювачі ANG-2300 збуджують шумові віброколивання в огороджувальних конструкціях, забезпечуючи при цьому мінімальний рівень перешкод акустичного сигналу в приміщенні практично не впливає на комфортність проведення переговорів. Комплект поставки передбачає всі необхідні установчі елементи для монтажу віброперетворювачів.

DNG-2300 цілеспрямовано розроблений для забезпечення Вашого захисту від засобів і методів підслуховування що не підлягають виявленню традиційними методами апаратурного і фізичного пошуку.

Звук, проходячи через огороджувальні та вентиляційні конструкції, викликає їх вібрацію. Контактні мікрофони або прилади лазерного або мікрохвильового зондування активно використовують цю здатність звуку, вловлюючи вібрації вентиляційних каналів, водопроводу, будівель, стін, вікон, дверей, підлоги й ін. І перетворюючи їх назад в звук. Мікрофон може бути встановлений не обов'язково в тій же кімнаті, де проходить розмова, може бути вмонтований в огороджувальні конструкції. Це значно ускладнює їх пошук і виявлення. DNG-2300 призначений для нейтралізації таких приладів.

Технічні характеристики DNG-2300:

Діапазон акустичного шуму - 180 Гц ... 5,6 кГц.

Тип вібраційного випромінювача - TRANSDUCERS.

Тип акустичний випромінювача - SPEAKERS.

Межі регулювання вихідної напруги - 0 ... 12 В.

Мінімальний опір навантаження - 8 Ом.

Опір одного випромінювача - 8 Ом.

Кількість підключаються випромінювачів на один блок - до 24.

Живлення 12-18 В постійного струму; мережа 220 В, 50 Гц через адаптер.

На теперішній час актуальним є також застосування глушилок бездротових закладних пристроїв. Наприклад "Піранья X16-5G" (рис.2.11).

Рис. 2.11 Блокатор бездротового зв’язку «Піранья X16-5G».

Цей пристрій живиться із мережі 220 В також він може живитися від мережі автомобіля 12 В вимикання та вмикання здійснюється по інфрачервоному каналі стійкому від радіочастотних перешкод .

Ефективність даного пристрою залежить від декількох факторів: відстані до джерела випромінювання відстань яку охоплює пристрій 125 метрів, відстань до приймача сигналів, а також залежно від того як спрямовані антени пристрою.

Пристрій має 16 антен для більш високої завади сигналам він був виконаний за принципом, що кожен з модулів призначений для блокування безпровідного каналу передачі в рамках одного з вище зазначених стандартів (табл. 2.1).

Таблиця 2.1

Діапазон частот електромагнітної завади

Діапазон частот (МГц)	Стандарт передачі інформації	Вихідна потужність не менше	
		Вт	дБм
925-960	GSM-900	3	+31
1805-1880	DCS-1800	3	+31
2110-2170	UMTS, 3G	3	+31
869-894	CDMA850	3	+31
463-467	CDMA450	4	+36
2400-2483,5	WIFI, BLUETOOTH, ZIGBEE	1	+27
1575,42-1605	GPS, Galileo, GLONASS	4	+36
1598-1606	GLONASS	3	+31
430-440	Діапазон який не потребує ліцензування	3	+31

Ефективність даного пристрою залежить від декількох факторів: відстані до джерела випромінювання відстань яку охоплює пристрій 30 метрів, відстань до приймача сигналів, а також залежно від того як спрямовані антени пристрою [12].

На зображеннях зображений зеленим кольором спектр пристроїв зв’язку , а червоним спектр завад пристрою (рис.2.12) .

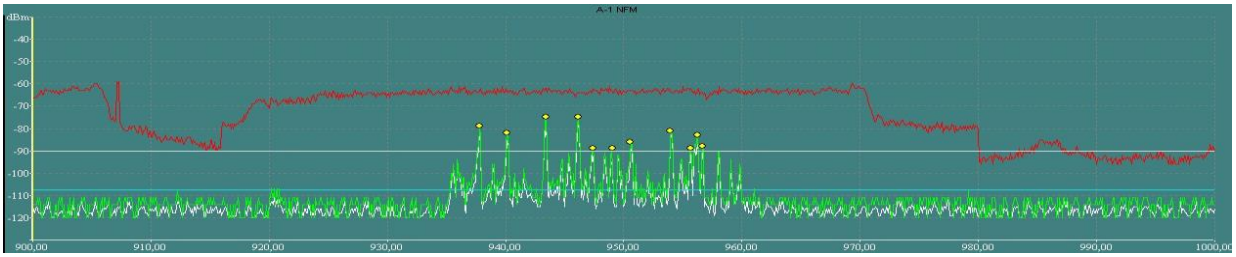


Рис 2.12 Діапазон Gsm-900 925-960MHz

Комплекс віброакустичного захисту PIAC-2ГС. Для захисту об'єктів інформатизації та протидії технічним засобам перехоплення мовної інформації

(стетоскопи, спрямовані і лазерні мікрофони, виносні мікрофони) по віброакустичних каналах (наведення мовного сигналу на стіни, підлогу, стелю приміщень, вікна, труби опалення, вентиляційні короба і повітряна звукова хвиля).

Рис. 2.13 Комплекс віброакустичного захисту РІАС-2ГС

Має два 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.

Вібровипромінювачі для зашумлення поділяються на два види: магнітодинамічні і п'єзокристалічні.

Конструкція магнітодинамічного датчика нагадує конструкцію звукового динаміка, у якого замість дифузора масивна платформа. Корпус датчика нагвинчується на штирьове кріплення жорстко, яке за допомогою холодного зварювання вмуровано в стіну. Цим забезпечується високий коефіцієнт корисної дії передачі коливань датчика в захищену стіну. Магнітодинамічні датчики добре відтворюють коливання в мовному діапазоні частот, генератори для спільної з ними роботи легко реалізуються на інтегральних підсилювачах, живлення датчиків низьковольтне.

До недоліків конструкції магнітодинамічних датчиків можна віднести високе енергоспоживання, необхідність узгодження по опору з виходом

генератора, наявність рухомих механічних частин, що веде до обмеженого ресурсу роботи і підвищеного шуму в роботі.

Конструкція п'єзокристального датчика складається з циліндричного металевого корпусу, всередині якого розміщений п'єзокристал. В даному випадку використовується зворотне властивість матеріалу. Якщо на п'єзокристал подати напругу, він почне стискатися. Таким чином, при подачі на кристал шумового сигналу він передає коливання корпусу датчика, а той в свою чергу через кріплення - в стіну. Способи кріплення у обох видів датчиків однакові. До переваг такого типу датчиків можна віднести малі габарити, мале енергоспоживання, відсутність рухомих елементів, внаслідок чого - підвищений ресурс роботи і низька гучність при роботі.

До недоліків даного типу датчиків треба віднести перевищення резонансної частоти кристалу мовного діапазону, високі напруги, в наслідок чого є більш складною реалізацією конструкції генератора.

До водопровідних труб датчики кріпляться за допомогою хомутів, на стекла вікон датчики клеяться.

Радіус дії датчиків, як правило, не перевищують величини 1,5-2 м При зашумленні всіх площин, труб, скла приміщення доводиться застосовувати велику кількість датчиків, крім того, для створення більш комфортних умов експлуатації датчики треба розташовувати якомога ближче один до одного і використовувати їх на малих потужностях. В результаті число датчиків ще збільшується. Через велику кількість датчиків, а отже, і збільшення застосовуваних генераторів віброакустичного захисту приміщень, таку системи є одним з найдорожчих видів захисту.

Прилад ANG-2 (рис. 2.14) призначений для захисту периметра приміщення від прослуховування [16].. З його допомогою можна виключити прослушки периметра шляхом зняття інформації з вікон, підвісних стель, ніш, повітропроводів і междверных прорізів. Краща ціна і хороша комплектація дозволяє придбати і ефективно використовувати ANG-2 будь-якої організації і приватній особі.

Рис. 2.14 Прилад віброакустичного захисту ANG – 2/

Двоканальний генератор шуму ANG-2 забезпечує генерацію акустичної мовоподібної перешкоди в діапазоні частотного спектра від 200 Гц до 6,2 кГц. Потужність завадового сигналу на кожному з виходів може регулюватися незалежно резисторами на задній стінці приладу. Виріб не створює перешкод пристроїв побутової електроніки. Рівень завадового акустичного сигналу, практично не впливає на комфортність проведення переговорів. У приладі використовуються два некорельованих джерела шуму, що виключають можливість відновлення мови методом фільтрації.

Технічні дані і характеристики ANG-2:

- кількість незалежних каналів: 2;
- спектр мовоподібної та шумової перешкоди: 220 Гц - 6,2 кГц;
- діапазон регулювання вихідного рівня: 42 дБ;
- мінімальна навантаження: 2 Ом;
- потужність вихідного сигналу: 2х8 Вт;
- кількість пьєзовипрмінювачів для віконних прорізів, що підключаються на один канал: до 24;
- кількість акустичних випромінювачів, що підключаються на один канал: до 8.
- електроживлення: 12 В, 3А (блок живлення в комплекті).

Висновок по розділу.

Встановлено, що найпоширенішими засобами прихованого отримання акустичної інформації є закладні пристрої, електронні та лазерні стетоскопи, спрямовані мікрофони.

Методи захисту акустичної інформації поділяються на активні та пасивні.

Засобами активного захисту акустичної інформації є акустичні та віброакустичні генератори білого шуму, радіоглушилки.

Розділ 3.
ТЕХНОЛОГІЯ ЕФЕКТИІНОГО ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ

Як показано у п. 2.1 є пасивні і активні методи забезпечення потрібного рівня розбірливості акустичної інформації у режимних об’єктах. Пасивні спрямовані на ослаблення акустичних сигналів, що циркулюють безпосередньо у приміщенні, активний захист реалізується різного роду генераторами перешкод, пристроями придушення.

Пасивні засоби захисту виділених приміщень. В основі пасивних засобів захисту інформації лежить зниження співвідношення сигнал/шум у можливих місцях перехоплення інформації за рахунок зниження рівня інформативного сигналу.

При виборі конструкцій, що обгороджують виділені приміщення, у процесі проектування необхідно керуватися наступними правилами:

- у якості перекриття рекомендується використати акустично неоднорідні конструкції;
- у якості підлоги доцільно використати конструкції на пружній основі або конструкції, установлені на віброізолятори;
- стелі доцільно виконувати підвісними, звуковбирними зі звукоізолюючим шаром;
- у якості стін і перегородок краще використовувати багатошарові акустично неоднорідні конструкції із пружними прокладками (гума, пробка, і т.п.).

Якщо стіни і перегородки виконані одношаровими, акустично однорідними, то їх доцільно підсилювати конструкцією типу «плита на відкоси», установлюваної з боку приміщення.

Шибки бажано віброізолювати від рам за допомогою гумових прокладок. Доцільне застосування потрійного скління вікон на двох рамах, закріплених на окремих коробках. При цьому на зовнішній рамі встановлюються зближені стекла, а між коробками укладається звуковбирний матеріал.

Двері необхідно використовувати подвійні, з тамбуром, при цьому дверні коробки повинні мати вібраційну розв'язку друг від друга.

Звукоізоляція приміщень. Виділення акустичного сигналу на тлі природних шумів відбувається при певних співвідношеннях сигнал/шум. Роблячи звукоізоляцію, домагаються його зниження до межі, що утрудняє (виключного) можливість виділення мовних сигналів, що проникають за межі контрольованої зони по акустичному або віброакустичному (огороджуючи конструкції, трубопроводи) каналам.

Для суцільних, однорідних, будівельних конструкцій ослаблення акустичного сигналу, що характеризує якість звукоізоляції на середніх частотах, розраховується по формулі:

$$K_{or} = 20\log(q_{or}f) - 47.5 \text{ дБ},$$

де:

q_{or} – маса 1 м^2 огородження, кг;

f – частота звуку, Гц.

Тому що середній рівень гучності розмови, що відбуває в приміщенні, становить 50...60 дБ, і звукоізоляція виділених приміщень залежно від привласнених категорій повинна бути не менш норм, наведених у табл. 3.1.

Таблиця 3.1

Звукоізоляція виділеного приміщення

Частота, Гц	Звукоізоляція виділеного приміщення, дБ		
	1 к	2 к	3 к
500	53	48	43
1000	56	51	46
2000	56	51	46
4000	55	50	45

Для обрання пасивних заходів захисту проведено наступне дослідження.

Змонтована установка (рис. 3.1) для дослідження звукоізоляційних властивостей ряду матеріалів для тональних (синусоїдальних) сигналів.

Сигнал звукової частоти, створений генератором ГС посилюється підсилювачем звукової частоти ПЗЧ і відтворюється гучномовцем Г. Після проходження ним звукоізоляційного матеріалу ЗМ він сприймається мікрофоном МКФ, посилюється вимірювальним підсилювачем ВП та виводиться на осцилограф ОСЦ.

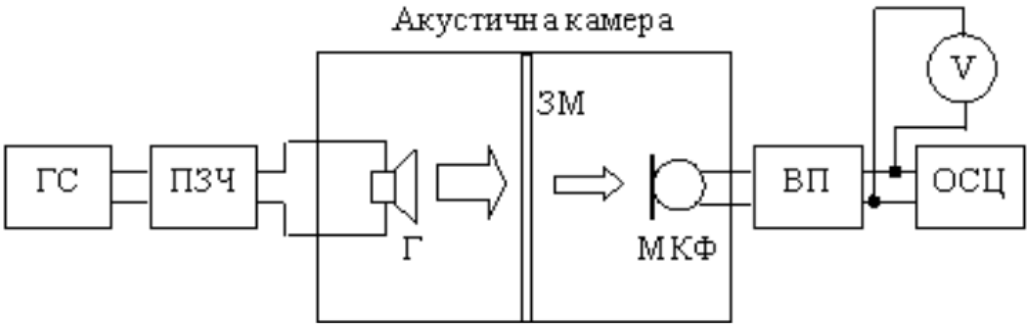


Рис. 3.1 Схема лабораторної установки

Звукоізолююча властивість зразка матеріалу характеризується величиною звукоізоляції R , яка в даному випадку визначалась як різниця рівнів звукового тиску на вході мікрофона, виміряних при відсутності –Lp та при наявності +Lp звукоізолюючого матеріалу:

$$R = L_{p-} - L_{p+}$$

Якщо врахувати, що рівень звукового тиску на вході мікрофона:

$$L_p = 20\lg\frac{p}{p_0}$$

а вимірювана осцилографом вихідна напруга:

$$U_{\text{вих}} = p \cdot S_{\text{м}} \cdot k_{\text{ВП}}$$

де:

p – значення звукового тиску на вході мікрофона, Па;

$p_o = 2\ 10^{-5} \cdot$ Па – звуковий тиск, що відповідає порогу чутності;

Sм - чутливість мікрофона, мВ/Па;

$k_{ВП}$ - коефіцієнт підсилення вимірювального підсилювача,

то:

$$R = 20\lg\frac{p_-}{p_+} = 20\lg\frac{U_{\text{вих}-}}{U_{\text{вих}+}}$$

Рівні сигналу вимірювались на середньогеометричних частотах 125, 250, 500, 1000, 2000, 4000, 8000 Гц октавних смуг мовного діапазону частот. Рівень гучності на вході мікрофона при відсутності звукоізоляційного матеріалу задавався близько 75 дБ, що відповідає гучній розмові.

Отримані частотні характеристики досліджуваних матеріалів наведено на рис.3.2. В області низьких частот у однорідних матеріалів звукоізоляція мало змінюється, в області середніх – відбувається постійне підвищення коефіцієнта с підвищенням частоти, але в області високих частот коефіцієнт звукоізоляції зменшується доволі швидко. Високі звукоізоляційні характеристики має гіпсокартон, проте в області низьких частот у нього спостерігається різке ослаблення звукоізоляції, що характерно для багатошарових матеріалів. В області високих частот його звукоізоляційні властивості практично стабільні.

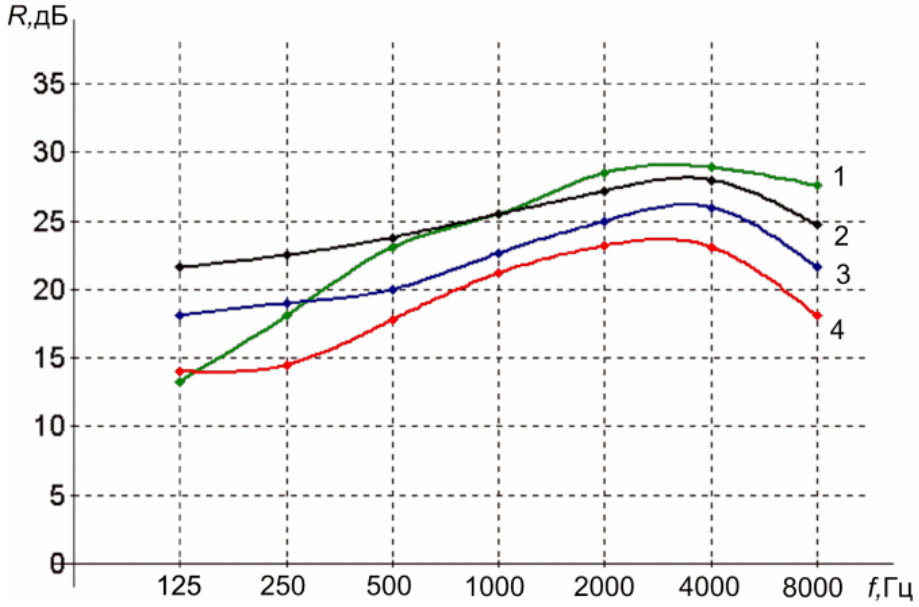


Рис. 3.2 Частотні характеристики звукоізоляції зразків матеріалів: 1 – гіпсокартону; 2 – сталі; 3 – скла; 4 – ламінованого ДВП

Таке дослідження було проведено для конкретних архітектурних конструкцій об’єкту інформаційної діяльності. Встановлено наступнк.

Самими слабкими ізолюючими якостями володіють двері (табл. 3.2) і вікна (табл. 3.3).

Таблиця 3.2

Звукоізоляція дверей

Тип	Конструкція	Звукоізоляція (дБ) на частотах, Гц					
		125	250	500	1000	2000	4000
Щитові двері,	Без прокладки	21	23	24	24	24	23
облицьовані фанерою із двох сторін	Із прокладкою з пористої гуми	27	27	32	35	34	35
Типові двері П-327	Без прокладки	13	23	31	33	34	36
	Із прокладкою з пористої гуми	29	30	31	33	34	41

У тимчасово використовуваних приміщеннях застосовують складні екрани, ефективність яких з урахуванням дифракції становить від 8 до 10 дБ.

Застосування звуковбирних матеріалів, що перетворять кінетичну енергію звукової хвилі в теплову, має деякі особливості, пов'язані з необхідністю створення оптимального співвідношення прямого і відбитого від перешкоди акустичних сигналів.

Надмірне звукопоглинання знижує рівень сигналу, великий час реверберації приводить до погіршення розбірливості мови. Значення ослаблення звуку огородженнями, виконаними з різних матеріалів, наведені в табл. 3.4.

Рівень сигналу за перешкодою R_{or} оцінюється виразом:

$$R_{or} = R_c + 6 + 10\log S_{or} - K_{or} \quad \text{дБ}$$

де:

R_c – рівень мовного сигналу в приміщенні, дБ;

S_{or} – площа огородження, м^2;

K_{or} – коефіцієнт поглинання матеріалу огородження, дБ.

Таблиця 3.3

Звукоізоляція вікон

Схема скління	Звукоізоляція (дБ) на частотах, Гц					
	125	250	500	1000	2000	4000
Одинарне скління:						
- товщина 3 мм	17	17	22	28	31	32
- товщина 4 мм	18	23	26	31	32	32
- товщина 6 мм	22	22	26	30	27	25
Подвійне скління з повітряним проміжком:						
57 мм (товщина 3 мм)	25	22	33	35	32	37
90 мм (товщина 3 мм)	21	29	38	44	40	46
57 мм (товщина 4 мм)	21	31	38	46	39	45
90 мм (товщина 4 мм)	25	33	41	47	48	48

Таблиця 3.4

Ослаблення звуку

Тип огородження	Коефіцієнт поглинання ($К_{ог}$) на частотах, Гц					
	125	250	500	1000	2000	4000
Цегельна стіна	0,024	0,025	0,032	0,041	0,049	0,07
Дерев'яна оббивка	0,1	0,11	0,11	0,08	0,082	0,11
Скло одинарне	0,03	0,028	0,027	*0,025	0,02	0,017
Штукатурка вапняна	0,025	0,04	0,06	0,085	0,043	0,058
Повсть (товщина 25 мм)	0,18	0,36	0,71	0,8	0,82	0,85
Килим з ворсом	0,09	0,08	0,21	0,27	0,27	0,37
Скляна вата (товщиною 9 мм)	0,32	0,4	0,51	0,6	0,65	0,6
Бавовняна тканина	0,03	0,04	0,11	0,17	0,24	0,35

Звукоізолюючі кабіни каркасного типу забезпечують ослаблення до 40 дБ, безкаркасного - до 55 дБ.

Із наступного можна зробити висновок, що для більш якісного захисту пасивними засобами потрібно ретельно підходити до вибору матеріалів, які будуть подавляти рівні гучності розмови в приміщенні. В таблиці 3.1 наведено якою повинна бути звукоізоляція виділених приміщень залежно від привласнених категорій при частоті Гц від 500-4000 [16]..

Стосовно звукоізоляції дверей, їх слід вибрати із прокладкою з пористої гуми, а саме: типові двері П-327, які вказані в таблиці 3.2.Вони володіють найбільш високими звукоізоляційними характеристиками.

У таблиці 3.3 наведено, що для якісної звукоізоляції вікон потрібно вибирати подвійне скління з повітряним проміжком -90 мм (товщина 4 мм), тому що воно володіє більшою звукоізоляційною характеристикою. Також ослаблення звуку залежить від того, які на об’єкті стіни, чи зроблена звукоізоляція приміщення та який коефіцієнт поглинання матеріалу.

Віброакустичний канал витоку інформації утворюють: джерела конфіденційної інформації (люди, технічні пристрої), середовище поширення (повітря, що обгороджують конструкції приміщень, трубопроводи), засоби отримання.

Для захисту приміщень застосовують генератори білого або рожевого шуму і системи вібраційного зашумлення, укомплектовані, як правило, електромагнітними і п'єзоелектричними віброперетворювачами.

Якість цих систем оцінюють перевищенням інтенсивності впливу, що маскує, над рівнем акустичних сигналів у повітряному або твердому середовищах.

Найкращі результати дає застосування коливань, які маскують близький по спектральному складу інформаційний сигнал. Шумовим такий сигнал не являється, крім того, розвиток методів шумоочищення в деяких випадках дозволяє відновлювати розбірливість мови до прийнятного рівня при значному (20 дБ і вище) перевищенні шумової перешкоди над сигналом. Отже, для ефективного маскування перешкода повинна мати структуру мовного повідомлення. Слід також зазначити, що через психофізіологічні особливості сприйняття звукових коливань людиною спостерігається асиметричний вплив коливань, що маскують. Воно проявляється в тім, що перешкода робить відносно невеликий вплив на маскуючі звуки, частота яких нижче її власної частоти, але сильно затрудняє розбірливість більше високих по тоні звуків. Тому для маскування найбільш ефективні низькочастотні шумові сигнали [9].

У більшості випадків для активного захисту повітряних каналів використовують системи віброзашумлення, до виходів яких підключають гучномовці. Так, у комплекті системи віброакустичного захисту DNG-2300 (фірма REI) поставляється акустичний випромінювач TRANSDUCERS. Однак застосування динаміків створює не що тільки маскує ефект, але і перешкоди нормальній повсякденній роботі персоналу в захищеному приміщенні.

Генератор електромагнітного шуму Піранья Х16-5G широкого діапазону у невеликому замкнутому просторі створює перешкоду потужністю до 16 Вт, що достатньо для придушення сигналів радіо закладних пристроїв, у тому числі й тих, що використовують традиційні цифрові стандарти..

Ефективність систем і пристроїв віброакустичного зашумлення визначається властивостями застосовуваних вібродатчиків які трансформують

електричні коливання в пружні коливання (вібрації) твердих середовищ. Якість перетворення залежить від реалізованого фізичного принципу, конструктивно-технологічного рішення і умов узгодження вібродатчика із середовищем.

Як було відзначено, джерела шумового сигналу повинні мати частотний діапазон, що відповідає ширині спектра мовного сигналу (300 ...9000 Гц), тому особливу важливість здобуває виконання умов узгодження перетворювача в широкій смузі частот. Умови широкосмугового узгодження з конструкціями, що обгороджують, що мають високий акустичний опір (цегельна стіна, бетонне перекриття) щонайкраще виконуються при використанні вібродатчиків з високим механічним імпедансом рухливої частини, якими на сьогоднішній день є п'єзокерамічні перетворювачі.

Під час роботи вібродатчиків виникають паразитні акустичні шуми, що вносять дискомфорт і нормальні умови, що порушують, умови праці в захищеному приміщенні.

Основним джерелом паразитних акустичних шумів є вібродатчик.

Експлуатаційно-технічні параметри деяких сучасних систем віброакустичного зашумлення наведені у табл. 3.5 [17].

Через частотну залежність акустичного опору матеріальних середовищ і конструктивних особливостей віброперетворювачів на деяких частотах не забезпечується необхідне перевищення інтенсивності перешкоди, що маскує, над рівнем наведеного в конструкції, що обгороджує, сигнал.

Збільшення потужності перешкоди створює підвищений рівень паразитного акустичного шуму, що викликає дискомфорт у працюючих у приміщенні людей. Це приводить до відключення системи в найбільш відповідальні моменти, створюючи передумови до витоку конфіденційних відомостей.

Таблиця 3.5

Системи вібро-акустичного зашумлення

Характеристика	ANG-2	PIAC – 2ГС	DNG-2300
Кількість незалежних генераторів	1	1	1
Робочий діапазон частот, кГц	0,22 - 6,2	0,25 - 5,0	0,18 - 5,6
Наявність еквалайзера	Є	Є	Є
Максимальна кількість вібродатчиків	24	24	TRANSDUCERS – 24
Ефективний радіус дії стінних вібродатчиків на перекритті товщиною 0,25 м, м	Не менш 6	Не менш 6	Не менш 5
Ефективний радіус дії віконних вібродатчиків на склі товщиною 4 мм, м	Не менш 1,5	Не менш 1,5	Не менш 1,5
Потужність акустичного каналу	8 Вт	4 Вт	8 Вт
Габарити вібродатчиків, мм	Ø40x30, Ø50x39, Ø33x8	Ø40x30, Ø50x39, Ø33x8	Ø100x38
Можливість акустичного зашумлення	Є	Є	Є

Оптимальні параметри перешкод. При застосуванні активних засобів необхідна для забезпечення захисту інформації величина співвідношення сигнал/шум досягається за рахунок збільшення рівня шумів у можливих крапках перехоплення інформації за допомогою генерації штучних акустичних і вібраційних перешкод. Частотний діапазон перешкоди повинен відповідати середньостатистичному спектру мови у відповідності з вимогами керівних документів.

У зв'язку з тим, що мова – шумоподібний процес зі складної (у загальному випадку випадкової) амплітудною і частотною модуляцією, найкращою формою що маскує перешкідний сигнал є також шумовий процес із нормальним законом розподілу щільності ймовірності миттєвих значень (тобто «білий» або «рожевий» шум).

Спектр перешкоди в загальному випадку повинен відповідати спектру сигналу, що маскує, але з обліком того, що інформаційна насиченість різних

ділянок спектра інформативного сигналу не однакова, для кожної октавної смуги встановлена своя величина перевищення перешкоди над сигналом. Нормовані відносини сигнал/шум в октавних смугах для кожної категорії виділених приміщень приводяться в керівних документах. Такий диференційований підхід до формування спектра перешкоди дозволяє мінімізувати енергію перешкоди, знизити рівень паразитних акустичних шумів при виконанні норм захисту інформації. Така перешкода є оптимальною.

Слід зазначити, що кожне приміщення і кожен елемент будівельної конструкції мають свої індивідуальні амплітудно-частотні характеристики поширення коливань. Тому при поширенні форма спектра первинного мовного сигналу змінюється відповідно до передатної характеристики траєкторії поширення. У цих умовах для створення оптимальної перешкоди, необхідне коректування форми спектра перешкоди у відповідності її спектром інформативного сигналу в крапці можливого перехоплення інформації.

Рекомендації щодо побудови системи захисту акустичної інформації на ОІД.

Виходячи з проведеного дослідження можливостей пасивних та активних засобів захисту акустичної інформації розроблено рекомендації по побудові системи захисту інформації від витоку акустичним каналом

Рекомендації приведено у таблицях 3.6 – 3.8. Рекомендації розроблено для об’єктів першої, другої та третьої категорій відповідно до НД ТЗІ 1.6 – 005-2013 та НД ТЗІ 1.5 – 005-2013.

Розробка рекомендацій ґрунтується на якісні вербальній оцінці активних та пасивних засобів захисту інформації [18].

Таблиця 3.6

Система захисту для ОІД 3–ої категорії

Елемент системи захисту	Варіанти системи захисту	
Двері	Щитові двері, облицьовані фанерою із двох сторін	Типові двері П-327
Вікна	Одинарне скління: товщина 3 мм товщина 4 мм товщина 6 мм	Одинарне скління: товщина 3 мм товщина 4 мм товщина 6 мм
Стіни	Цегельна стіна з дерев'яною обивкою, або цегельна стіна з штукатуркою вапняною	Цегельна стіна з бавовняною тканиною
Активний захист	Генератор шуму РІАС - 2ГС	Генератор шуму РІАС - 2ГС

Таблиця 3.7

Система захисту для ОІД 2–ої категорії

Елемент системи захисту	Варіанти системи захисту	
Двері	Типові двері П-327	Щитові двері, облицьовані фанерою із двох сторін
Вікна	Подвійне скління з повітряним проміжком: 57 мм (товщина 3 мм) 90 мм (товщина 3 мм)	Одинарне скління: товщина 3 мм товщина 4 мм товщина 6 мм
Стіни	Цегельна стіна з дерев'яною оббивкою, або цегельна стіна з штукатуркою вапняною	Цегельна стіна зі штукатуркою вапняною
Активний захист	Генератор шуму DNG 2300	Генератор шуму DNG 2300

Таблиця 3.8

Система захисту для ОІД 1–ої категорії

Елемент системи захисту	**Варіанти системи захисту**	
Двері	Типові двері П-327	Типові двері П-327
Вікна	Подвійне скління з повітряним проміжком: 57 мм (товщина 4 мм) 90 мм (товщина 4 мм)	Подвійне скління з повітряним проміжком: 57 мм (товщина 4 мм) 90 мм (товщина 4 мм)
Стіни	Цегельна стіна зі скляною ватою (товщиною 9 мм	Цегельна стіна з бавовняною тканиною та килим з ворсом
Активний захист	Генератор шуму ANG- 2	Генератор шуму ANG-2

Висновок по розділу.

Проаналізовані захисних можливостей активних та пасивних засобів захисту інформації.

Активні засоби (генератори віброакустичного шуму) відрізняються потужністю акустичного та віброакустичного сигналів на виході, кількістю кінцевих пристроїв, а відповідно і параметрами приміщення, що захищається.

Серед пасивних засобів застосовуються архітектурно-будівельні заходи по таким напрямам: двері, вікна, стіни, підлога.

Розроблені рекомендації по застосуванню активних та пасивних засобів для облаштування об’єктів першої, другої та третьої категорій.

Запропоновані рекомендації дозволять забезпечити безпеку акустичної інформації у режимних приміщеннях.

ВИСНОВКИ

Несанкціоноване отримання акустичної інформації на об’єктах інформаційної діяльності є суттєвою загрозою.

У дипломній роботі встановлено, що фізично, шляхами витоку інформації є: повітряний, віброакустичний, параметричний, оптико-електронний.

Встановлено, що найбільш часто використовуваними засобами несанкціонованого отримання акустичної інформації є: закладні пристрої, лазерний та електронний стетоскопи, метод високочастотного нав’язування.

Критерієм розбірливості мови являється словісна розбірливість мови.

Для захисту інформації від витоку акустичним каналом застосовуються пасивні та активні методи.

Реалізацією активних методів є застосування приладів віброакустичного захисту та акустичного зашумлення приміщення.

Реалізацією пасивних методів захисту є використання архітектурно-будівельних засобів.

Під час дослідження встановлені чисельні показники якісті захисту акустичної інформації активними та пасивними засобами.

Розроблені рекомендації по комплексному використанню активних та пасивних засобів захисту акустичної інформації на ОІД першої, другої та третьої категорій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про інформацію» № 2657-XII від 2 жовтня 1992 року

2.Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII

3. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

4. Хорошко В.А., Чекатков А.А. Методи та засоби захисту інформації. – К.: ЮНИОР, 2013. – 504 с.

5. Сучасний стан захисту інформації. [Електронний ресурс]– URLhttp://www.immsp.kiev.ua/publications/articles/2009/2009_2/Litvinov_02_2009.pdf

6. Хорошко В.А., Чекатков А.А. Методи та засоби захисту інформації. – К.: ЮНІОР, 2013. – 504

7. Системи та пристрої інформаційної безпеки. Навчальний посібник / під ред. проф. В.А. Хорошко / Співавтори: А.П. Провозин, О.В. Рибальский, В.А.Хорошко, Д.В.Чирков. – К.: ДУІКТ, 2007.

8. Інформаційна безпека та кібербезпека держави. / Н.М. Титова, Н.М. Рідей, В.П. Настрадін, М.М. Присяжнюк, С.М. Мамченко, С.В. Артюх, Р.О. Яворська / К.: Ліра-К, 2024 – 224 с.

9. Інформаційна безпека / О.І. Фармагей, Оксана Карпович, В.В. Остроухов, М. М. Присяжнюк, М.М. Чеховська / К.:Ліра-К, 2021 – 230 с.

10. Технічний захист інформації / В.М. Богуш, В.Д. Бровко, О.С. Кобус, В.Д. Козюра / Ліра-К, 2022 – 508 с.

11. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. – К.: ДУТ. – 2020. – 126 с.

12. Термінологічний довідник з питань технічного захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

13. Головань С.М. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.

14. Кібербезпека: сучасні технології захисту / Остапов С.Е., Євсеєв С.П., Король О.Г. / К.: Новий Світ -2000, 2023 – 678 с.

15.https://xn--80adgebslrpy8u.com.ua/henerator-akustychnoho-shumu-statsionarnyi-rias2hs/

16. https://ibughunter.com.ua/dng-2300/?srsltid=AfmBOopSLNJKSP4oJwkar0doHsgl0mweztQ2LIPkpmAXz2jKvS8QkEjV

17.https://ibughunter.com.ua/uk/ang-2/?srsltid=AfmBOoruCI1rD2KRP45ci9AvpQskg7CHWR_LaTvlEovFYSLHGCEuqRMT

18. Технології захисту інформації / Остапов С.Е., Євсеєв С.П., Король О.Г. / К.: Новий Світ-2000, 2020 – 500.

19. Конструкції будинків і споруд. Звукоізоляція огороджувальних конструкцій. Методи оцінювання: ДСТУ Б В.2.6-85:2009. - К. : Міжрегіонбуд, 2010. – (Національний стандарт України).

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ТЕХНОЛОГІЯ ЕФЕКТИВНОГО ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ НА РЕЖИМНИХ ОБ’ЄКТАХ

Кваліфікаційна робота здобувача освітнього ступеня «МАГІСТР»
Андрій ОПАЛЬКО
Спеціальність 125 – Кібербезпека та захист інформації
Керівник: к.т.н., доц. Ігорь ІВАНЧЕНКО
Київ – 2025

Слайд 1

АКТУАЛЬНІСТЬ РОБОТИ

2

• зростання ролі акустичних каналів як джерела витоку інформації на режимних об’єктах
• необхідність протидії підслуховуванню, диктофонам, радіозакладкам, стетоскопам і лазерним засобам зняття інформації
• потреба у комплексному поєднанні активних і пасивних методів захисту акустичної інформації

Об’єкт / предмет
процес захисту інформації / захист акустичної інформації

Слайд 2

ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

3

• РОЗДІЛ 1. Проаналізовано загрози акустичній інформації та основні шляхи її втрати.
• РОЗДІЛ 2. Досліджено активні й пасивні методи та засоби захисту акустичної інформації.
• РОЗДІЛ 3. Розроблено технологію ефективного захисту акустичної інформації на режимних об’єктах.
• ВИСНОВКИ. Сформовано практичні рекомендації щодо підвищення захищеності мовної інформації.

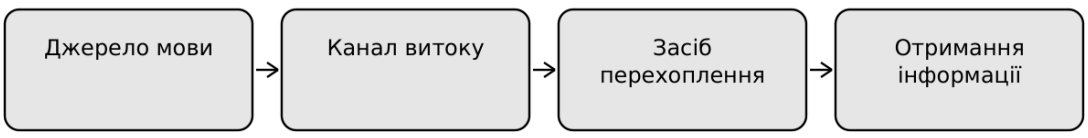
Слайд 3

ПЕРШИЙ РЕЗУЛЬТАТ

4

ЗАГРОЗИ АКУСТИЧНІЙ ІНФОРМАЦІЇ

• підслуховування та несанкціонований запис мовної інформації
• використання закладних пристроїв, диктофонів, стетоскопів, лазерних систем
• перехоплення через двері, вікна, стіни, вентиляційні канали та інженерні комунікації



Слайд 4

ПЕРШИЙ РЕЗУЛЬТАТ

5

КЛАСИФІКАЦІЯ АКУСТИЧНИХ КАНАЛІВ ВИТОКУ

Повітряні поширення звуку через повітряне середовище	Вібраційні передавання структурного звуку через конструкції	Оптико-електронні лазерне зняття коливань з поверхонь
Акусто-електричні мікрофонний ефект у технічних засобах	Параметричні модуляція випромінювань під дією мовного сигналу	Закладні пристрої приховане встановлення засобів перехоплення

Слайд 5

ДРУГИЙ РЕЗУЛЬТАТ

6

ЗАСОБИ ПРИХОВАНОГО ОТРИМАННЯ АКУСТИЧНОЇ ІНФОРМАЦІЇ

- портативні диктофони та мікрофонні системи прихованого запису
- радіозакладки, мережеві, телефонні та інфрачервоні закладки
- спрямовані мікрофони та електронні стетоскопи
- лазерні акустичні системи для дистанційного зняття мовної інформації

Слайд 6

ДРУГИЙ РЕЗУЛЬТАТ

7

КРИТЕРІЙ РОЗБІРЛИВОСТІ МОВНОГО ПОВІДОМЛЕННЯ

• основним показником захищеності акустичної інформації є словесна розбірливість мови W
• при зниженні W ускладнюється складання довідки про зміст перехопленої розмови
• оцінювання виконується з урахуванням спектральних рівнів мовлення та шуму

$$E = Bp - Bш \rightarrow W = f(E)$$

Слайд 7

ДРУГИЙ РЕЗУЛЬТАТ

8

АКТИВНІ МЕТОДИ ЗАХИСТУ

• акустичне та віброакустичне маскування мовного сигналу
• створення шумового поля у контрольованому приміщенні та на огороджувальних конструкціях
• застосування генераторів шуму, випромінювачів і вібровипромінювачів
• зниження розбірливості перехопленого мовного повідомлення до безпечного рівня

Слайд 8

ДРУГИЙ РЕЗУЛЬТАТ

9

ПАСИВНІ МЕТОДИ ЗАХИСТУ

Звукоізоляція ущільнення дверей, вікон, вентиляції	Конструкційний захист посилення стін, перегородок, стель
Організаційні заходи регламент доступу та контроль приміщення	Пошук закладок обстеження приміщень і технічних засобів

Слайд 9

ТРЕТІЙ РЕЗУЛЬТАТ

10

ТЕХНОЛОГІЯ ЕФЕКТИВНОГО ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ

Слайд 10

ТРЕТІЙ РЕЗУЛЬТАТ

11

ПОБУДОВА КОМПЛЕКСНОГО ЗАХИСТУ

• визначення контрольованої зони та потенційних місць перехоплення
• оцінювання повітряних, вібраційних, електроакустичних і лазерних каналів
• розміщення засобів маскування на критичних напрямках витоку
• періодична перевірка рівня захищеності після впровадження заходів

Слайд 11

ТРЕТІЙ РЕЗУЛЬТАТ

12

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ

Рівень	Словесна розбірливість	Оцінка
Високий ризик	75-98 %	розмова добре відновлюється
Середній ризик	40-75 %	можлива коротка анотація
Низький ризик	10-40 %	визначаються лише окремі слова
Захищений стан	< 10 %	зміст розмови не встановлюється

Слайд 12

ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

13

• організувати регулярне обстеження режимних приміщень на наявність каналів витоку
• поєднувати пасивну звукоізоляцію з активним акустичним і віброакустичним маскуванням
• здійснювати контроль доступу до приміщень перед проведенням закритих нарад
• проводити періодичну перевірку ефективності захисту за показником розбірливості мовлення

Слайд 13

ВИСНОВКИ

14

• проаналізовано основні шляхи втрати акустичної інформації та засоби її прихованого отримання
• узагальнено активні й пасивні методи захисту акустичної інформації
• обґрунтовано використання словесної розбірливості як критерію ефективності захисту
• запропоновано технологію підвищення ефективності захисту акустичної інформації на режимних об’єктах

ДЯКУЮ ЗА УВАГУ!

Слайд 14