

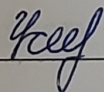
Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

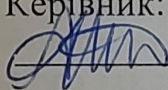
БАКАЛАВРСЬКА ДИПЛОМНА РОБОТА

на тему:

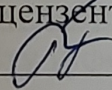
"Розробка пристрою захисту інформації від зйому мікрофоном направленої дії
акустичним каналом"

Виконав: студент 4 курсу, гр. 2КІТС-206
спеціальності 125– Кібербезпека
Освітня програма – Кібербезпека
інформаційних технологій та систем
(шифр і назва напрямку підготовки, спеціальності)

 Усач М. В.
(прізвище та ініціали)

Керівник: к.т.н., доц., доцент каф. МБІС
 Шиян А. А.
(прізвище та ініціали)

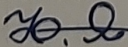
« 6 » сервіс 2024 р.

Рецензент: к.т.н., доц., доцент каф. ОТ
 Тарновський М. Г.
(прізвище та ініціали)

« 6 » сервіс 2024 р.

Допущено до захисту

Голова секції УБ кафедри МБІС

д.т.н., проф. Яремчук Ю.Є. 

« 6 » сервіс 2024р. 

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти І-й (бакалаврський)

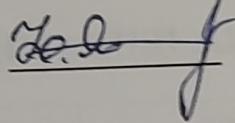
Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітньо-професійна програма - Кібербезпека інформаційних технологій та систем

ЗАТВЕРДЖУЮ

Голова секції УБ, кафедра МБІС



д.т.н., проф. Яремчук Ю.Є.

“ 22 ” березня 2024 р.

ЗАВДАННЯ

на бакалаврську дипломну роботу студенту

Усачу Миколі Васильовичу

(прізвище, ім'я, по-батькові)

1. Тема роботи "Розробка пристрою захисту інформації від зйому мікрофоном направленої дії акустичним каналом"

Керівник роботи к.т.н., доц., доцент каф. МБІС Шиян А. А

(прізвище, ім'я, по-батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “ 11 ” березня 2024 року № 80

2. Термін подання студентом роботи 11.06.2024 р.

3. Вихідні дані до роботи Набір даних каналів витоку інформації акустичними каналами для розробки пристрою захисту інформації акустичним каналом.

4. Зміст текстової частини:

1. Аналіз каналів витоку акустичної інформації

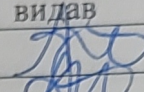
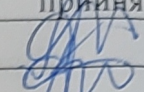
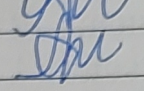
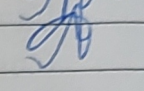
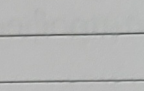
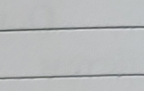
2. Розробка пристрою захисту інформації від зйому мікрофоном направленої дії

3. Моделювання роботи пристрою

5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень)

Презентація у форматі PowerPoint з ілюстраціями структурної схеми приладу та скріншотами моделювання схеми приладу

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ I	доцент Шиян А. А		
Розділ II	доцент Шиян А. А		
Розділ III	доцент Шиян А. А		

7. Дата видачі завдання 22 березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва та зміст етапу	Термін виконання		Примітка
		початок	закінчення	
1	Визначення напрямку бакалаврської дипломної роботи, формулювання теми	22.03.2024	24.03.2024	
2	Постанова задач	25.03.2024	29.03.2024	
3	Аналіз предметної області обраної теми	01.04.2024	07.04.2024	
4	Дослідження інформаційних джерел	08.04.2024	12.04.2024	
5	Розробка структурної схеми	13.04.2024	19.04.2024	
6	Вибір бази елементів	20.04.2024	27.04.2024	
7	Моделювання роботи приладу	02.05.2024	15.05.2024	
8	Оформлення матеріалів до захисту БДР	20.05.2024	30.05.2024	
9	Переддипломний захист			
10	Захист бакалаврської дипломної роботи			

Студент

Керівник роботи

(підпис)

(прізвище та ініціали)

(підпис)

(прізвище та ініціали)

Усач М. В.

Шиян А. А.

АНОТАЦІЯ

У даній бакалаврській дипломній роботі розроблено пристрій захисту інформації від зйому мікрофоном направленої дії акустичним каналом. В роботі проаналізовано існуючі методи захисту від акустичного шпигунства та визначено технічні аспекти для розробки пристрою, який ефективно захищати конфіденційні дані від несанкціонованого доступу через акустичний канал. У цій роботі наведено рекомендації щодо запобігання витоку інформації акустичними та віброакустичними шляхами в приміщеннях і офісах, а також приклади вимог до рівня захищеності об'єкта.

ANNOTATION

In this bachelor's thesis, a device for protecting information from being captured by a microphone directed by an acoustic channel is developed. The paper analyzes existing methods of protection against acoustic espionage and defines technical aspects for the development of a device that effectively protects confidential data from unauthorized access through an acoustic channel. This work provides recommendations for preventing information leakage through acoustic and vibroacoustic pathways in premises and offices, as well as examples of requirements for the object's security level.

Зміст

ВСТУП	3
1. АНАЛІЗ КАНАЛІВ ВИТОКУ АКУСТИЧНОЇ ІНФОРМАЦІЇ	5
1.1 Акустичний канал витоку інформації	5
1.2 Віброакустичний канал витоку інформації.....	11
1.3 Електроакустичний канал витоку інформації.....	15
1.4 Лазерно-акустичний канал витоку інформації	20
1.5 Методи захисту інформації від витоку акустичними каналами	23
1.5.1 Активний захист інформації.....	26
1.5.2 Пасивний захис інформації.....	28
1.6 Висновки та постановка задач.....	31
2. РОЗРОБКА ПРИСТРОЮ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ЗЙОМУ МІКРОФОНОМ НАПРАВЛЕНОЇ ДІЇ.....	33
2.1 Розробка структурної схеми пристрою	33
2.2 Вибір бази елементів	37
2.3 Вибір джерела живлення.....	42
2.4 Висновки до розділу	43
3. МОДЕЛЮВАННЯ РОБОТИ ПРИСТРОЮ.....	45
3.1 Обґрунтування вибору елементів пристрою	45
3.2 Моделювання роботи підсилювача на транзисторі	48
3.3 Моделювання роботи генератора шуму	51
3.4 Висновки до розділу	57
ВИСНОВКИ	59
Перелік посилань	60
Додаток А. Технічне завдання.....	63
Додаток Б. Ілюстраційний матеріал.....	67
Додаток В. Протокол перевірки на антиплагіат	74

ВСТУП

Актуальність задачі. У сучасному світі інформація стає все більш цінним активом, а отже, зростає потреба в її захисті. Одним з найпоширеніших методів витоку інформації є перехоплення інформації спрямованими мікрофонами через акустичні канали. Це може призвести до серйозних наслідків, таких як втрата конфіденційних даних, вимагання та промислове шпигунство.

З поширенням технологій збору аудіоінформації зростає загроза порушення конфіденційності даних через запис акустичних каналів спрямованими мікрофонами. Це вимагає розробки ефективних заходів захисту інформації для виявлення та блокування несанкціонованого доступу до акустичних даних.

Також зростає усвідомлення важливості захисту інформації не лише у корпоративному секторі, а й у державних установах та приватних домогосподарствах. Успішна розробка пристрою, здатного блокувати перехоплення інформації по акустичних каналах, внесе значний внесок у підвищення загальної безпеки інформаційного простору.

Метою роботи є розробка пристрою для захисту інформації від перехоплення спрямованими мікрофонами через акустичні канали за рахунок генератора білого шуму, що підвищує ефективний захист від цього виду шпигунства та гарантує конфіденційність і безпеку оброблюваної інформації.

Для досягнення мети роботи необхідно вирішити наступні завдання

1. Проаналізувати методи та засоби для захисту інформації від зйому мікрофоном направленої дії акустичним каналом.
2. Удосконалити метод захисту інформації від перехоплення спрямованими мікрофонами через акустичні канали за рахунок створення генератора шуму.
3. Спроекувати дослідний зразок пристрою.

Об'єктом дослідження є акустичний канал витоку інформації та методи його захисту від зняття мікрофоном.

Ця робота спрямована на створення пристрою для захисту інформації від прослуховування за допомогою генератора шуму, щоб запобігти витоку

конфіденційних даних через акустичні канали.

Предметом дослідження є пристрій захисту інформації від зняття мікрофоном направленої дії акустичним каналом.

У цьому дослідженні буде розглянуто поточний стан та проведено аналіз існуючих методів захисту. На основі цього аналізу буде створено пристрій, який можна використовувати в різних сферах, де конфіденційність має вирішальне значення.

Новизна даного дослідження полягає в розробці пристрою захисту інформації, заснованого на принципі активного захисту. Цей пристрій має такі переваги: адаптованість до різних умов, простота застосування.

Практична цінність цієї роботи полягає у створенні пристрою безпеки, який може бути використаний в офісах, комерційних приміщеннях і громадських будівлях для забезпечення конфіденційності мовлення та запобігання несанкціонованому доступу до критично важливої інформації. Такі пристрої безпеки можуть стати необхідним компонентом систем безпеки в різних сферах діяльності, знижуючи ризик витоку конфіденційної інформації та забезпечуючи захист приватного життя.

Тому ця робота важлива не тільки для конкретного користувача, але і для суспільства в цілому, сприяючи створенню більш безпечного інформаційного середовища.

1. АНАЛІЗ КАНАЛІВ ВИТОКУ АКУСТИЧНОЇ ІНФОРМАЦІЇ

1.1 Акустичний канал витоку інформації

Фізичний шлях від джерела акустичних сигналів до злоумисника - це акустичний канал, що передає інформацію за рахунок механічних коливань

Тіла та механізми, які здійснюють вібрацію або коливання, наприклад голосовий апарат людини, рухоме обладнання, телефонні апарати тощо. Звукові коливання, що виникають від голосу людини та інших звуків, утворюють акустичні хвилі. Ці хвилі поширюються у просторі і взаємодіючи з відповідними перешкодами, викликають у них перемінний тиск (двері, вікна, стіни, підлога, різні прилади), приводячи їх у коливальний режим. Впливаючи на спеціальні прилади (мікрофони), звукові коливання створюють у них відповідні електромагнітні хвилі, які передаються на відстань і несуть у собі створену звуковими коливаннями інформацію.

Акустичні канали утворюються шляхом перехоплення мовних сигналів (акустичних полів) з ОІД акустичними мікрофонами направленої дії чи акустичними антенами засобів технічної розвідки, що встановлюється за межами КЗ в зоні видимості з вікон (з інших отворів). (Рисунок 1.1)[1]

- за рахунок «мембранного ефекту». Так званий «мембранний ефект» обумовлений коливанням тонких (відносно довжини) і, як правило відносно легких, елементів огорожувальних конструкцій (віконного скла, фанерних, гіпсокартонних, пластикових перегородок тощо), здатних прогинатися під дією звуку;

- через тріщини, отвори, щілини та інші акустичні отвори, тобто прямим розповсюдженням акустичних коливань;

- за рахунок перетворення акустичних коливань в віброакустичні, а потім знов в акустичні.

У даному випадку частина енергії акустичних коливань (частина відбивається), падаючи на поверхню огорожувальної конструкції, перетворюється на віброакустичну, тобто в коливання твердих частинок матеріалу без перенесення

речовини. Подолавши огорожувальну конструкцію, частина енергії віброакустичних коливань (частина відбивається) перетворюється на акустичну і випромінюється у вигляді акустичних коливань.

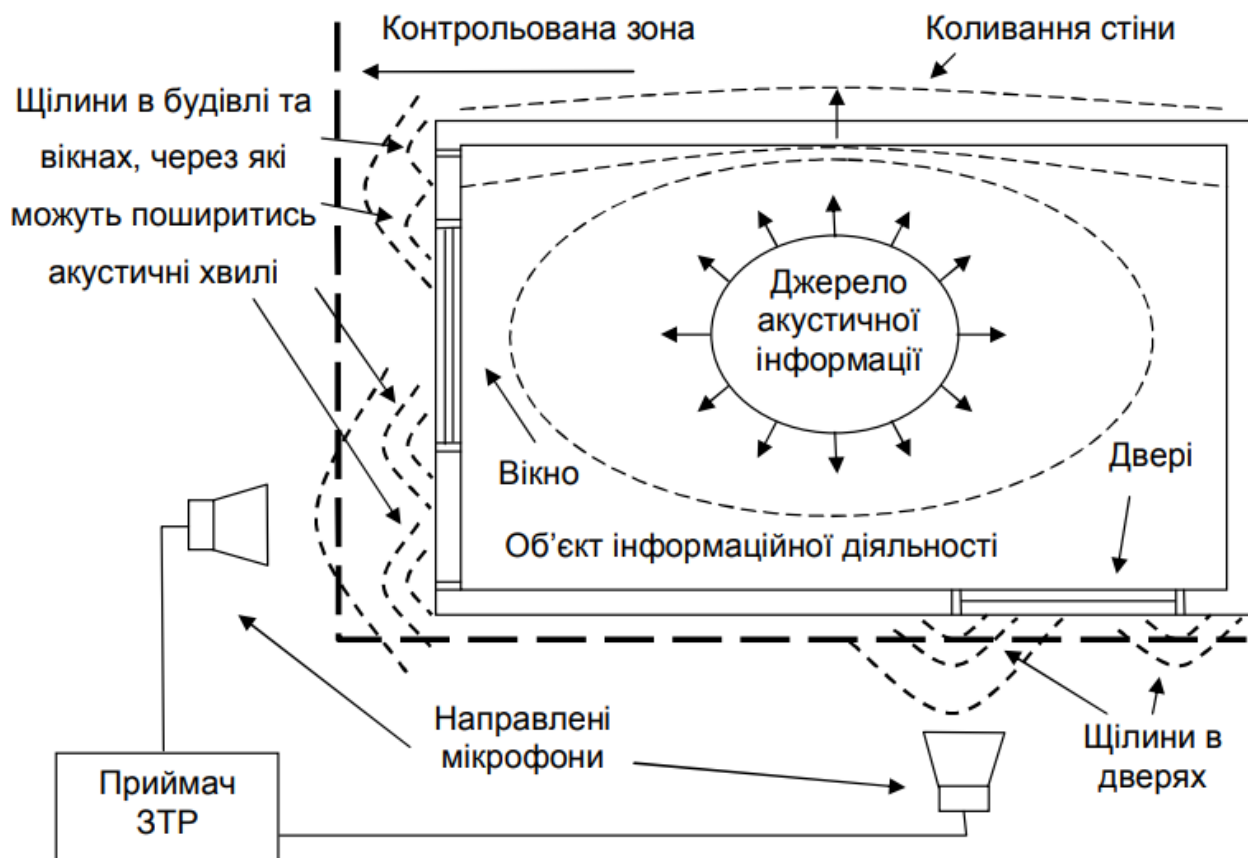


Рисунок 1.1 – акустичні канали витоку інформації[1].

Найбільш корисними методами з перерахованих вище є акустичний моніторинг і перехоплення переговорів в приміщеннях зв'язку. Ці методи використовують спеціальні технічні засоби для нелегального отримання інформації. Для отримання конфіденційних відомостей зазначені методи найбільш інформативними - акустичний контроль та перехоплення переговорів у приміщеннях зв'язку

Для перехоплення та реєстрації акустичної інформації існує величезний набір засобів розвідки: мікрофони, електронні стетоскопи, акустичні закладки, спрямовані й лазерні мікрофони, апаратури магнітного запису. Набір акустичних засобів розвідки, які використовуються для вирішення конкретного завдання, істотно залежить від можливості доступу агента в контрольоване приміщення або до

зацікавлених осіб.

Якщо доступ до об'єкта контролю є постійним, можна використовувати простий невеликий мікрофон зі з'єднувальною лінією в сусідню кімнату для запису і прослуховування акустичної інформації. Такий мікрофон, діаметром 2,5 мм, може вловити звичайний людський голос з відстані 20 метрів.

Якщо зловмисники не мають постійного доступу до об'єкта, але можуть здійснювати короточасні візити під різними приводами, для акустичної розвідки використовуються невеликі диктофони або магнітофони, замасковані під повсякденні предмети, такі як книги, письмове приладдя або коробки з-під сигарет. Крім того, диктофон може бути у будь-кого з присутніх на закритому засіданні. У цьому випадку часто використовуються виносні мікрофони, заховані під одягом або замасковані під годинники, авторучки, гудзики тощо.

Сучасні диктофони - це більше, ніж просто пристрої для запису голосу. Вони оснащені низкою функцій, необхідних для збору інформації[1].

Ось деякі з основних особливостей сучасних диктофонів:

- Тривалий час запису: можна записувати довгі розмови, від 30 хвилин до 7-8 годин.
- Система акустичного захоплення: UAX, UA5 - автоматично починає запис при виявленні звуку, заощаджуючи час і пам'ять.
- Автоматичний реверс: коли запис з одного боку закінчено, стрічка автоматично перевертається для безперервного запису.
- Відображення мітки дати і часу: записує дату і час запису, що полегшує пошук потрібної інформації.
- Дистанційне керування: дозволяє керувати диктофоном на відстані, що робить його більш зручним у використанні.

Електронні стетоскопи:

У випадку, якщо зловмисникам не вдається потрапити на об'єкт, але є доступ до сусідніх приміщень, вони можуть використовувати електронні стетоскопи. Електронні стетоскопи – Ці пристрої, оснащені п'єзоелементом, здатні підсилити

акустичний сигнал, що дозволяє відслідковувати звуки через стіни, підлогу та стелю, навіть якщо вони звучать далеко.

Основні особливості електронних стетоскопів такі:

- Чутливий елемент: п'єзоелектричний елемент, який підсилює акустичний сигнал.
- Коефіцієнт підсилення: до 20 000-30 000 разів, що дозволяє вловлювати навіть слабкі звуки.
- Дальність дії: від 1 метра крізь бетонні стіни.

Акустичні закладки:

Акустичні закладки - це несанкціоновані пристрої, що розміщуються в приміщеннях або транспортних засобах для перехоплення акустичної інформації.

Паралельно з диктофонами для перехоплення акустичної інформації використовуються акустичні закладки, які розміщуються на несанкціонованих об'єктах і в транспортних засобах. Для передачі перехопленої інформації використовуються різні канали зв'язку, включаючи радіо- та оптичні канали, а також силові та слабкоструміві комунікації.

Найпоширенішим типом є радіозакладки, які можна класифікувати за кількома критеріями:

- Використовуваний частотний діапазон
- Потужність випромінювання: низька потужність - до 10 мВт; середня потужність - від 10 мВт до 100 мВт; висока потужність - понад 100 мВт;
- Тип використовуваного сигналу: прості сигнали (АМ, РМ), складні сигнали (ІFR, шумоподібні сигнали);
- За методом модуляції: модуляція несучої, модуляція проміжної частоти;
- За методом стабілізації частоти: нестабілізовані, стабілізовані контуром (м'який канал), стабілізовані кварцом (кварцові);
- За дизайном: у вигляді окремого модуля, замаскованого під різні предмети (авторучка, калькулятор, подовжувач, дерев'яний брусок).

Радіозакладки можуть передавати дані на великі відстані - від десятків метрів

(наприклад, авторучка може передавати до 50 метрів) до одного кілометра. За допомогою ретрансляторів цю відстань можна збільшити до десятків кілометрів. Для забезпечення конфіденційності радіозакладки можуть бути оснащені різними технологіями, такими як акустичне придушення, пакетна передача і шифрування сигналу.

Мережеві закладки використовуються для передачі інформації через електромережу. Вони можуть бути встановлені на різних пристроях, таких як електричні розетки, подовжувачі, пілоти та прилади, або підключені безпосередньо до електромережі. Основним недоліком є обмежений діапазон передачі даних, зазвичай від одного будівельного майданчика до підстанції. Однак він має перевагу в тому, що його важко виявити. Для отримання інформації використовуються спеціальні приймачі.

Акустична інформація перехоплюється за допомогою так званих "телефонних вух" і передається по телефонній лінії. Зателефонувавши за відповідним номером, агент може почути, що відбувається в приміщенні, навіть якщо він перебуває в іншому місті.

Окремі датчики вібропреобразовувачів також можуть виходити з ладу або втрачати зв'язок, що може знизити ефективність захисту.

Класифікація пристроїв захисту інформації від мікрофонного прослуховування для акустичного каналу витоку може бути здійснена за наступними критеріями:

1. Тип захисту:

- **Активний захист:** Включає в себе використання активних методів, таких як створення шумових акустичних перешкод або використання акустичних віброакустичних пристроїв.
- **Пасивний захист:** Базується на використанні пасивних методів, таких як використання акустичних матеріалів з підвищеною звукоізоляцією або акустичних фільтрів.

2. Призначення:

- **Пристрої для промислового використання:** Розроблені для захисту

конфіденційної інформації у промислових або комерційних об'єктах.

- **Пристрої для особистого використання:** Призначені для захисту приватної інформації в особистих або домашніх умовах.

3. Характеристики пристроїв:

- **Рівень шуму:** Мінімальний та максимальний рівні шуму, що може бути згенерований пристроєм.
- **Частотний діапазон:** Діапазон частот, у якому працює пристрій, що визначає його ефективність у блокуванні звукових сигналів.
- **Енергоспоживання:** Потужність, споживана пристроєм під час роботи.

Зважаючи на широкий спектр пристроїв для захисту інформації від мікрофонного прослуховування, наведемо декілька прикладів в таблиці 1

Таблиця 1.1 - основні характеристики деяких пристроїв акустичного маскування[2]

Назва пристрою	Тип захисту	Рівень шуму (дБ)	Частотний діапазон (Гц)	Енергоспоживання (Вт)	Метод захисту	Посилання
AN-G-2000 Acoustic Noise Generator	Активний	До 85	300 - 4000	10	Шумове маскуванн я	[2]
VNG-006 Voice Noise Generator	Активний	До 90	200 - 6000	15	Шумове маскуванн я	[2]
Baron Acoustic White Noise Generator	Активний	До 88	400 - 5000	12	Шумове маскуванн я	[2]
Zaslon Acoustic Shielding Material	Пасивний	До 30	-	-	Акустичні перешкоди	[2]

Виходячи з даних таблиці можна зробити наступні висновки:

AN-G-2000 Acoustic Noise Generator: Забезпечує рівень шуму до 85 дБ у частотному діапазоні 300-4000 Гц з енергоспоживанням 10 Вт і компактними розмірами 150x100x50 мм. Цей пристрій ефективно маскує звукові сигнали в приміщенні.

VNG-006 Voice Noise Generator: Генерує шум до 90 дБ у ширшому частотному діапазоні 200-6000 Гц, споживаючи 15 Вт енергії. Розміри пристрою 180x120x60 мм. Вищий рівень шуму та ширший частотний діапазон роблять його ефективним для захисту різних типів приміщень.

Baron Acoustic White Noise Generator: Створює шум до 88 дБ у частотному діапазоні 400-5000 Гц з енергоспоживанням 12 Вт. Розміри пристрою 160x90x70 мм. Оптимальне співвідношення розмірів і ефективності для стандартних умов захисту.

Загальне порівняння пристроїв для захисту від прослуховування мікрофонів в акустичних каналах показує, що існують як активні, так і пасивні методи захисту. Активні пристрої, такі як генератори шуму, використовують маскування шуму для забезпечення швидкого та ефективного захисту. З іншого боку, пасивні методи, такі як акустичні перешкоди та шифрування, менш вразливі до виявлення і можуть виявитися більш економічними в довгостроковій перспективі.

1.2 Віброакустичний канал витоку інформації

Сутність акустовібраційних (віброакустичних) каналів витоку полягає в тому, що акустична хвиля небезпечного сигналу, впливаючи на поверхню твердого матеріалу (який є пружним середовищем), спричиняє його вібрацію - коливання молекул. Ці коливання можуть розповсюджуватись на значні відстані, залежно від густини матеріалу. Чим більша густина, тим далі може розповсюджуватись сигнал.

Наприклад на ОІД де озвучується інформація такими твердими тілами та пружними середовищами, є огорожувальні конструкції приміщення (стіни з дверям та вікнами, стеля, підлога) та всі інші предмети (система опалення, водопостачання та водовідведення, газопровід, тощо), що трапляються на шляху змінного акустичного тиску та які виходять за межі

ОІД, або мають щільний контакт з предметами за межами ОІД[1]. (Рис.1.2)

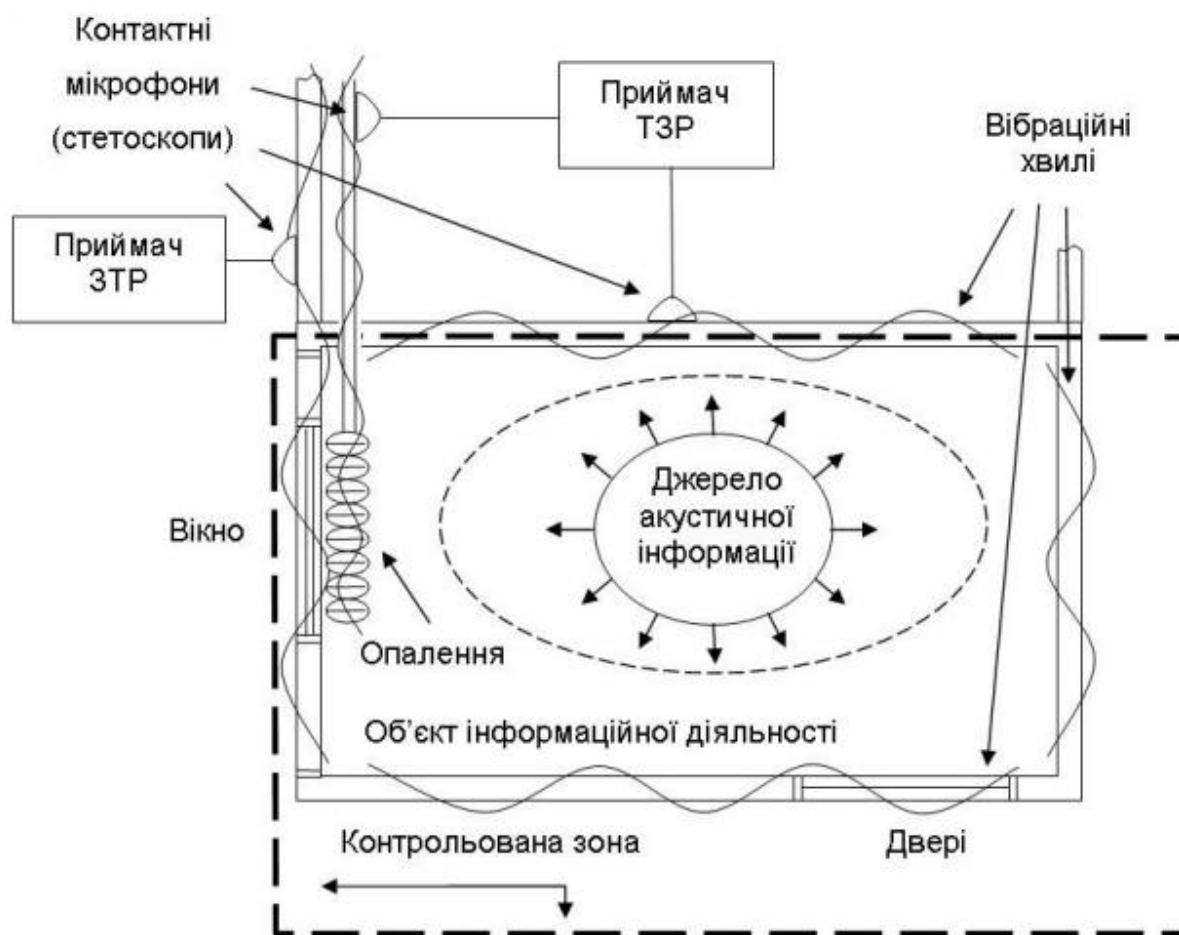


Рисунок 1.2 – Віброакустичний канали витоку інформації

По віброакустичному каналу також можливо перехоплення інформації з використанням ЗП. Для передачі інформації часто використовується радіоканал, тому такі пристрої часто називають радіостетоскопами. Можливе використання ЗП з передачею інформації по оптичному каналу в ближньому інфрачервоному діапазоні довжин хвиль, а також по ультразвуковому каналу (по інженерним комунікаціям).

Пристрої віброакустичного захисту призначені для захисту конфіденційних приміщень від зняття інформації через різні елементи, такі як шибки, стіни, системи вентиляції, труби опалення, двері тощо. Вони заважають можливому прослуховуванню за допомогою різних пристроїв, таких як дротяні мікрофони, звукозаписні пристрої, радіомікрофони і електронні стетоскопи, а також лазерні засоби зняття акустичної інформації через вікна і т.д.

Пристрої віброакустичного захисту:**Призначення:**

- Захист приміщень, де проводяться конфіденційні заходи, від витоку інформації через вікна, стіни, системи вентиляції, труби опалювання, двері та інші елементи конструкції.

Застосування:

- Запобігає прослуховуванню за допомогою:
 - Дротяних мікрофонів.
 - Звукозаписної апаратури.
 - Радіомікрофонів.
 - Електронних стетоскопів.
 - Лазерного знімання акустичної інформації з вікон.

Принцип дії:

- Внесення віброакустичних шумових коливань в елементи конструкції будівлі.

Конструкція:

- Блок формування і посилення шумового сигналу.
- Декілька акустичних і віброакустичних випромінювачів.

Генератор:

- Формує "білий шум" в діапазоні звукових частот.

Передача акустичних коливань:

- За допомогою п'єзоелектричних (на основі п'єзокераміки) або електромагнітних вібраторів з елементами кріплення.

Вимоги до випромінювачів:

- Конструкція і частотний діапазон повинні забезпечувати ефективну передачу вібрації.

Вібропреобразовувачі:

- Порушують шумові віброколивання в захищаючих конструкціях.
- Забезпечують мінімальний рівень перешкоджаючого акустичного сигналу в приміщенні.

- Практично не впливають на комфортність проведення переговорів.

Переваги:

- Ефективний захист від прослуховування.
- Мінімальний вплив на комфортність людей в приміщенні.
- Широкий спектр застосування.

Ці випромінювачі забезпечують ефективну передачу вібрації, щоб порушити акустичні сигнали у захищених конструкціях, зберігаючи при цьому комфортність переговорів.

Вибір пристрою віброакустичного захисту залежить від розмірів та конструкції приміщення, а також від очікуваного рівня загрози.

Для створення акустичних завад методом віброакустичного маскування використовують спеціальні генератори, що керують гучномовцями або вібраційними випромінювачами. Найчастіше для цього застосовують генератори шуму, що робить цей метод також відомим як акустичне зашумлення. Для формування шумових сигналів використовують різноманітні елементи, включаючи вакуумні, газорозрядні, напівпровідникові та цифрові пристрої[2].

Наразі існує багато систем віброакустичного маскування, таких як Заслон, Кабінет, Барон, Фон-В, VNG-006, ANG-2000, NG-101, АД-24, Г-002 та інші. Характеристики деяких з них подані в таблиці 2.

Таблиця 1.2 - основні характеристики деяких систем віброакустичного маскування

Характеристика	Модель		
	VNG-006DM	ANG-2000	Заслон-2М
Смуга частот ефективного захисту для перекриття товщиною 0,25 м,	0,25-5,0	0,25-5,0	0,1-5,0

Тип; принцип дії датчика	КВП-2, КВП-6, КВП-7; п'єзоелектричний	TRN-2000, електромагнітний	Електромагнітний
Ефективний радіус подавлення вібродатчика, встановленого на перекритті товщиною 0,25 м,	4	5	1,5
Особливості конструкції	Підключення спікера	Підключення спікера	Акустопуск. Адаптація до акустичного фону
Посилання	14	15	16

Отже, можна зробити такі висновки:

ANG-2000 виглядає найефективнішим з точки зору радіуса подавлення (5 м) і має порівняно широку смугу частот ефективного захисту (0,25-5,0 кГц), що робить його підходящим для великих приміщень.

VNG-006DM є досить ефективним з радіусом подавлення 4 метри і має п'єзоелектричні датчики, що може бути корисним у деяких специфічних випадках.

Заслон-2М виділяється своєю широкою смугою частот (0,1-5,0 кГц) і додатковими функціями адаптації до акустичного фону, хоча його ефективний радіус (1,5 м) значно менший, що може обмежувати його застосування у великих приміщеннях.

Кожна модель має свої переваги та недоліки, що дозволяє вибирати пристрій залежно від конкретних потреб захисту інформації та умов використання.

Для створення віброакустичних перешкод використовуються спеціальні генератори на основі електровакуумних, газорозрядних і напівпровідникових радіоелементів.

1.3 Електроакустичний канал витоку інформації

Акустоелектричний (електроакустичний) канал витоку інформації виникає при

перетворенні акустичного каналу в електричний.

Деякі елементи допоміжних технічних пристроїв і систем (ДТЗС), такі як трансформатори, котушки індуктивності, електромагніти у вторинних годинниках і телефонних дзвінках, мають здатність змінювати свої параметри (ємність, індуктивність і опір) під впливом акустичного поля, що генерується джерелом звукового сигналу[3].

Коли ці параметри змінюються, в цих елементах генерується електрорушійна сила (ЕРС) або модулюється струм, що проходить через них, у відповідь на зміни електричного поля.

ДТЗС, крім зазначених елементів, можуть містити безпосередньо акустoeлектричні перетворювачі. До таких відносяться деякі типи датчиків пожежної та охоронної сигналізації, гучномовці ретрансляційної мережі тощо. Ефект акустoeлектричного перетворення іноді називають «мікрофонним ефектом».

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

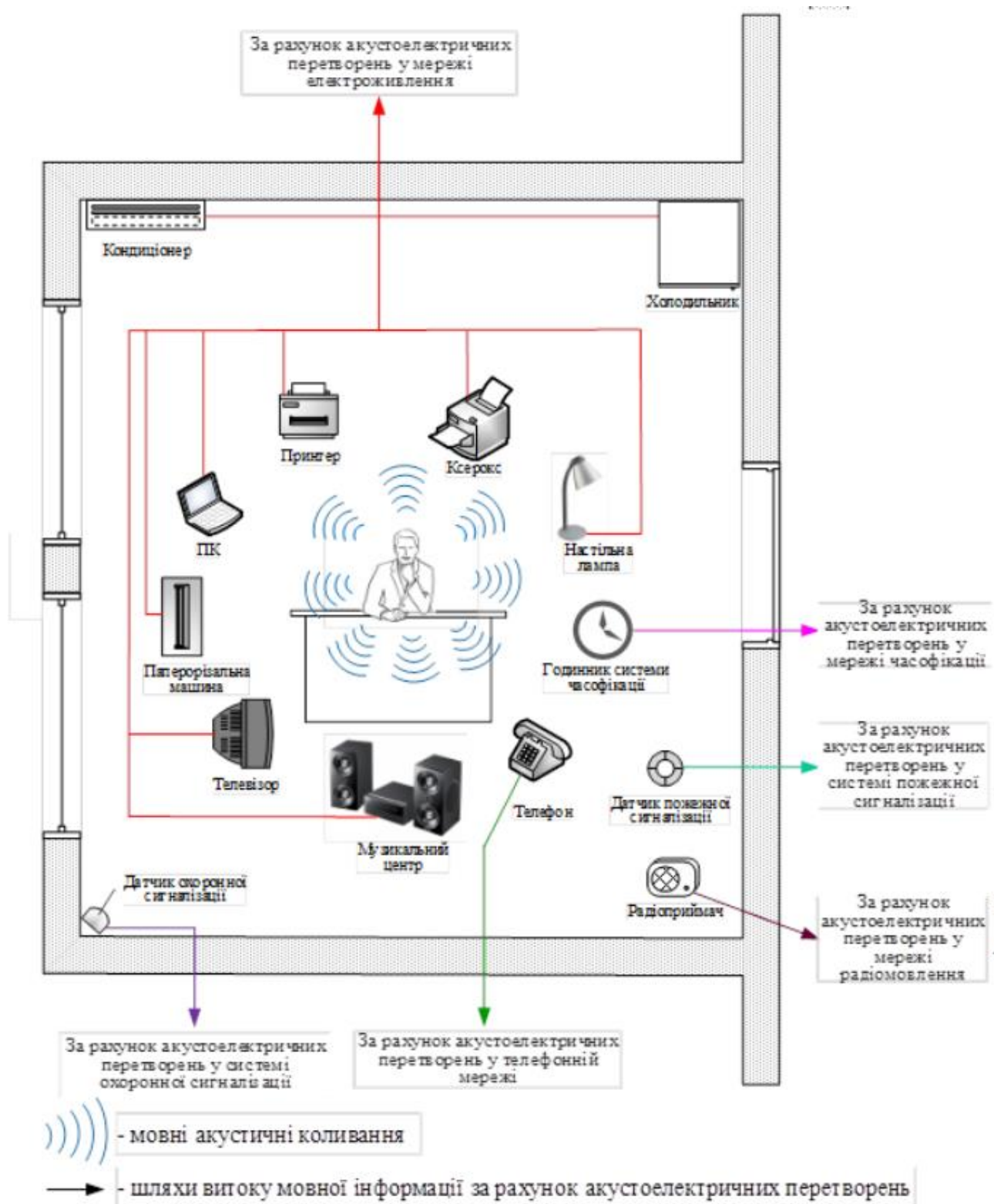


Рисунок 1.3 - Канали витоку акустичної інформації за рахунок акустоелектричних перетворювань[3].

Підключивши такі пристрої до з'єднувальних ліній телефонних апаратів з електромеханічними викличними панелями, можна прослуховувати розмови в приміщеннях, де встановлені ці апарати.

Технічний канал витоку інформації з використанням "електромагнітного впливу високої частоти" може бути реалізований шляхом несанкціонованого контактного введення струму високої частоти від генератора в лінію, функціонально пов'язану з нелінійним або параметричним елементом НВІС, де високочастотний канал модулюється інформаційним сигналом. Інформаційні сигнали в цих елементах з'являються в результаті акустоелектричного перетворення акустичних сигналів в електричні. Модульований сигнал відбивається від цих елементів і поширюється або випромінюється у зворотному напрямку.

Класифікація пристроїв захисту інформації від електроакустичного прослуховування може включати наступні категорії[3]:

Активний пристрій:

1. **Генератор електроакустичного шуму:** створює шумові сигнали у відповідному діапазоні частот і перекриває їх корисними сигналами.
2. **Електроакустичні перешкоди:** включають електронні пристрої, які перешкоджають передачі аудіоінформації по електроакустичних каналах.

Пасивні пристрої:

1. **Акустичний екран:** використовується для поглинання, відбиття або розсіювання звуку, знижуючи ефективність прослуховування.
2. **Акустичний фільтр:** блокує або фільтрує певну частоту або частотний діапазон, щоб звук не було чути.

Для порівняння технічних характеристик декількох пристроїв, наведено в таблиці 1.3

Таблиця 1.3 - основні характеристики деяких пристроїв електро-акустичного маскування.

Пристрій	Робоча частота	Гучність (дБ)	Дальність дії	Живлення	Додаткові функції	Посилання
White Noise Machine, Marpac Sound	60-80 Гц	50-70 дБ	2-3 метри	120 В	Регульована гучність	17
	100-	40-60 дБ	10-20	110-240 В	Підключення до	18

Masking System, Sound Machines	5000 Гц		метрів		мережі, настінний монтаж	
Speech Privacy System, Yamaha VSP-1	200-4000 Гц	55-75 дБ	10 метрів	100-240 В	Інтеграція з мережами зв'язку, програмовані налаштування	19
Noise Masking Generator, Cambridge Sound Management	125-5000 Гц	45-65 дБ	15-30 метрів	110-240 В	Зонування, підключення до систем будівлі	20

Аналізуючи ці характеристики, можна зробити наступні висновки:

Універсальність

Пристрої, такі як LectroFan і Magpas, відзначаються універсальністю завдяки широкому діапазону частот і можливості регулювання гучності. Це робить їх придатними як для індивідуального використання, так і для офісних приміщень.

Потужність і дальність дії

Cambridge Sound Management та Sound Machines є оптимальними для великих приміщень завдяки великій дальності дії та здатності створювати акустичні зони.

Спеціалізовані функції

Yamaha VSP-1 відзначається можливістю інтеграції з мережами зв'язку та програмованими налаштуваннями, що робить його особливо корисним у корпоративному середовищі.

Живлення

Більшість стаціонарних систем потребують живлення від мережі, тоді як портативні пристрої, як LectroFan, можуть працювати від USB, що додає зручності у використанні.

Отже, загалом вибір пристрою залежить від конкретних потреб: для індивідуального використання краще підходять портативні пристрої з широким діапазоном гучності, тоді як для великих офісів чи спеціалізованих середовищ оптимальними є потужні системи з можливістю інтеграції та зонування.

1.4 Лазерно-акустичний канал витоку інформації

Лазерно-акустичні канали (ЛАК) - один з найновіших і найменш вивчених каналів витоку інформації. Він використовує лазерний промінь для вібрації тонких поверхонь, таких як вікна, стіни та меблі, і записує звук, що виникає при вібрації. Цей звук може містити конфіденційну інформацію, наприклад, звуки розмови людей або роботи комп'ютера.

Переваги

- Невидимість: лазерний промінь тонкий і невидимий, що ускладнює його виявлення.
- Відстань: лазер може працювати на великих відстанях до декількох сотень метрів.
- Спрямованість: лазерний промінь може бути сфокусований на певній точці, що робить його більш точним, ніж інші шляхи витоку інформації.

Недоліки

- Складність: вимагає складного апаратного і програмного забезпечення.
- Чутливість до вібрації: може бути чутливим до вібрацій від інших джерел, що може ускладнити запис інформації.
- Обмеження поверхні: може працювати лише на тонких, твердих поверхнях.

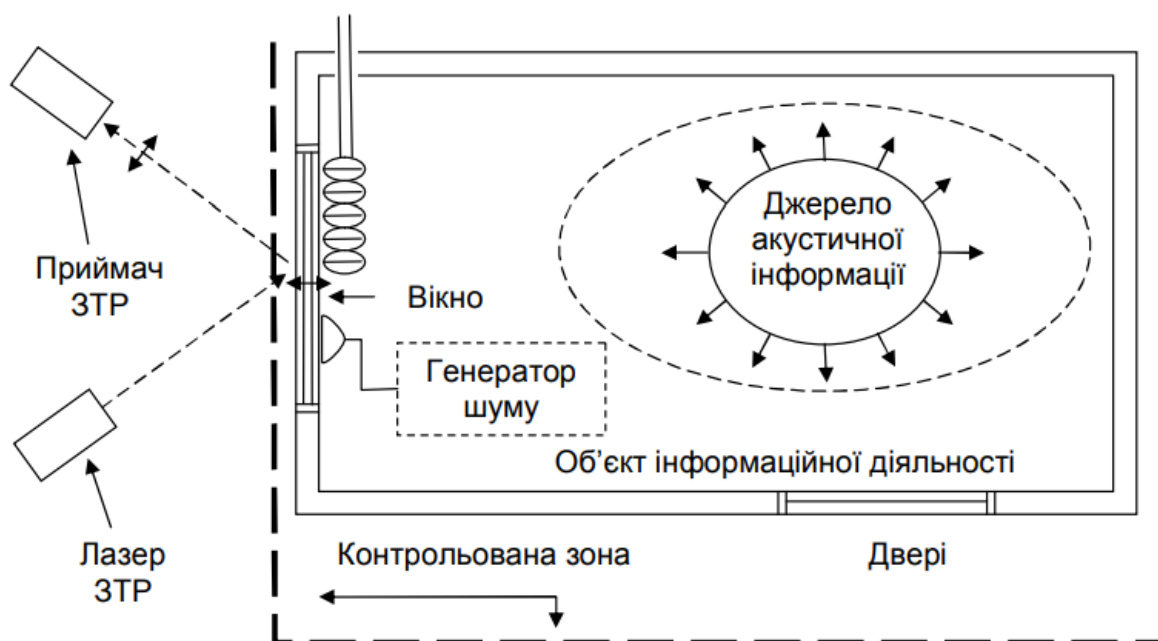


Рисунок 1.4 – Лазерно-акустичний канал витоку інформації.

Сутність акустооптоелектронних (лазерних акустичних) каналів витоку інформації полягає в такому. На ОІД, де озвучується інформація, під впливом небезпечного акустичного сигналу знаходяться усі предмети. Деякі предмети, що мають оптичні властивості віддзеркалення, приводяться до вібрації[3]. Такими предметами є скло вікна, дзеркало тощо. Вібрація таких предметів зв'язана з коливанням їх поверхні. Якщо ззовні ОІД на поверхню скла, дзеркала, що вібрують, спрямувати лазерний промінь, то він віддзеркалиться від поверхні у вигляді промінчика, модульованого тремтінням від сигналу вібрації, і розповсюджуватиметься далі (рис. 1.4). Тремтіння Віддзеркалений промінь може бути перехоплений противником, здійснена його демодуляція (виділене тремтіння) і відновлений початковий інформаційний мовний сигнал.

Для захисту від лазерно-акустичного прослуховування існують різні пристрої з різними технічними характеристиками. Характеристики деяких з них подані в таблиці 1.4.

Таблиця 1.4 - основні характеристики деяких пристроїв лазерно-акустичного маскування.

Пристрій	Частотний діапазон	Потужність лазера	Рівень звукового тиску (дБ)	Дальність дії (м)	Живлення	Додаткові функції	Посилання
LaserShield LMS-1000	100 Гц - 10 кГц	5 мВт	80-100	30	220В	Інтеграція з системами безпеки	21
SoundLaser SL-1	200 Гц - 20 кГц	10 мВт	75-95	50	12В	Портативний, керування з смартфона	22

Acousticom Model 2	150 Гц - 15 кГц	7 мВт	85-110	40	110-240В	Захист від зворотнього зв'язку	23
--------------------	-----------------	-------	--------	----	----------	--------------------------------	----

Отже, з даної таблиці можна зробити такі висновки:

LaserShield LMS-1000: цей пристрій працює в широкому діапазоні частот від 100 Гц до 10 кГц і використовує лазер потужністю 5 МВт. Воно забезпечує звуковий тиск 80-100 дБ і дальність дії до 30 метрів. Інтеграція з системою безпеки робить його ідеальним для професійного використання. Висока ціна відповідає його потужності та ефективності.

SoundLaser SL - 1: портативний пристрій з частотним діапазоном потужності лазера 200 Гц-20 кГц і потужністю 10 МВт. Звуковий тиск досягає 95 дБ, а дальність дії - 50 метрів. Можливість управління зі смартфона корисна для різних додатків. Його ціна робить його доступним варіантом для особистого користування.

Acousticom Model 2: пристрій з частотним діапазоном від 150 Гц до 15 кГц і потужністю лазера 7 МВт. Звуковий тиск досягає 110 дБ, а дальність дії - 40 метрів. Захист від зворотного зв'язку робить його надійним вибором для захисту конфіденційної інформації.

Кожен пристрій має свої унікальні методи захисту, які можуть бути вибрані в залежності від конкретних потреб і умов використання.

як пасивний захист від лазерних систем акустичної розвідки можна використати наступні заходи:

1. Маскування або заміна об'єктів з гладкою поверхнею, що можуть відбити лазерний промінь з найменшими шумами, викликаними нерівностями поверхні
2. Використання захисної плівки на вікна задля погіршення якості відбитого лазера
3. Перекриття виду зсередини, а саме використання щупких штори, щоб повністю закрити інтер'єр кімнати та поглинути звукові коливання

4. Перекриття вікна ззовні, а саме використання ролетів на зворотній стороні вікна, на які не впливатимуть небезпечні мовні сигнали з приміщення та що будуть перекривати віброуюче вікно.

1.5 Методи захисту інформації від витоку акустичними каналами

Для запобігання витоку звукової інформації акустичними та віброакустичними каналами вживаються заходи щодо виявлення каналу витоку. У більшості випадків зловмисники використовують пристрої з відповідними наворотами з метою несанкціонованого зняття інформації з приміщень.

Всю процедуру пошуку пристроїв можна розділити на кілька етапів:

- Фізичний обшук і візуальний огляд
- Виявлення пристроїв радіоперехоплення як електронних пристроїв;
- Виявлення шляхів витоку інформації

Фізичний пошук і візуальний огляд

Здійснюється шляхом огляду всіх предметів у контрольованій зоні, які є достатньо великими, щоб містити технічні засоби негласного отримання інформації (настільні пристрої, рамки для картин, телефони, квіткові горщики, книги, мережеві блоки живлення: комп'ютери, ксерокси, радіоприймачі тощо).

Фізичний обшук та візуальний огляд предметів здійснюється за допомогою спеціальних засобів відеоспостереження та металошукачів.

Основними приладами, що використовуються для виявлення приладів, є

- Польові індикатори
- Спеціальні радіоприймачі
- Програмно-апаратні комплекси радіоконтролю.
- Нелінійні радіолокатори.

Польові індикатори - це пристрої, які виявляють наявність пристроїв за допомогою радіовипромінювання. Індикатори або польові детектори - це найпростіший спосіб виявити використання радіопристроїв[4]. Вони являють собою менш чутливі приймачі, які можуть виявляти випромінювання радіопередавачів на дуже малих відстанях (10-40 см) і надійно розрізняти

"незаконні випромінювання" на тлі сильних "законних сигналів". Важливою перевагою детектора є те, що він може виявляти передавальні пристрої незалежно від використовуваної схеми модуляції. Основний принцип пошуку полягає у виявленні абсолютного максимального рівня випромінювання в приміщенні.

Іноді детектори використовуються в режимі сторожового сигналу. У цьому випадку, після повної перевірки відсутності в приміщенні пристроїв, рівень поля фіксується в певній точці приміщення (зазвичай це робочий стіл керівника або переговорна кімната) і пристрій переходить в режим очікування. При активації закладки (приблизно за 2 метри від датчика) індикатор подає сигнал про підвищення рівня електромагнітного поля. Однак при використанні бездротової закладки з дуже низьким рівнем електромагнітного поля слід враховувати можливість того, що датчик не зафіксує її активацію[4].

Радіоприймальний пристрій як детектор радіозакладок має задовольняти трьом основним умовам:

- * бути здатним перебудовуватися на робочу частоту пристрою, що потайки передає перехоплену інформацію, тобто контролювати великі набори частот шляхом перебудови від значення до значення одночасно у всьому діапазоні або за дуже короткий час (панорамний приймач)

- * можливість виділення потрібного сигналу залежно від характеристик сигналу і сигналу, що заважає (вибірковість за частотним спектром);

- * можливість демодуляції різних типів сигналів (видалення сигналів несучої частоти, перетворення корисних сигналів на сигнали низької частоти і демодуляція за допомогою детекторів, що відповідають типу використовуваної модуляції).

Слід зазначити, що дорогі попередні перевірки приміщень на наявність прослуховувальної апаратури і технічних каналів витоку інформації безглузді, якщо апаратуру вносять напередодні секретних перемовин або безпосередньо учасники переговорів.

Існує ціла низка обладнання для управління операціями службою безпеки перемовника. До них відносяться металодетектори і засоби виявлення працюючих диктофонів і підслуховуючих пристроїв, хоча таке обладнання часто дає помилкові

спрацьовування або має низький відсоток виявлення (особливо щодо диктофонів). Використовувати їх не завжди етично. Крім того, ми завжди повинні припускати, що "ворог" розумніший за нас і матиме при собі обладнання, навіть якщо воно вимкнене. Як уже зазначалося вище, необхідно також враховувати віброакустичні канали витоку звукової інформації та погану звукоізоляцію приміщень.

У світлі цього найнадійнішим заходом протидії несанкціонованому отриманню голосової інформації є запобігання запису переговорів та їхній ретрансляції з приміщення шляхом створення акустичного шуму або цілеспрямованого придушення.

Шляхи витоку голосової інформації можуть бути не тільки технічними, а й природними, такими як повітря, несучі конструкції, труби опалення та водопостачання, вентиляційні канали тощо.

Для запобігання витоку необхідно перекрити всі можливі шляхи і вивести з ладу пристрої перехоплення (мікрофони, спрямовані мікрофони, диктофони, стетоскопи, пристрої, що імплантуються, лазерні системи, інфрачервоні випромінювачі тощо).

Одним із найпоширеніших методів захисту є створення акустичних шумових завад, які забезпечують маскування інформаційного сигналу. Співвідношення шумового та інформаційного сигналу має або забезпечувати надійне приховування інформаційного сигналу, або знижувати його розбірливість до достатньої межі.

Для захисту від зйому мікрофоном направленої дії акустичним каналом можна використовувати методи захисту, які включають:

1.Створення шумових акустичних перешкод: Цей метод полягає у створенні шуму, який приховує або знижує чіткість мовлення, ускладнюючи запис. Шум може бути "білим", "пофарбованим" або "мовоподібним", залежно від спектральних характеристик приховуючого мовного сигналу.

2.Використання засобів захисту від вібраційних каналів: Це включає в себе використання генераторів шуму мовного діапазону, які супроводжуються віброперетворювачами, для створення шумових перешкод в стінах, вікнах та інженерних комунікаціях, що ускладнює запис мовлення.

3.Фізичний захист інфраструктури: Це включає в себе будівельні роботи з акустичного захисту, такі як встановлення шумопоглинаючих матеріалів та засобів у вікнах, стінах і трубопроводах, що зменшує передачу звукових сигналів.

Ці методи захисту допомагають утримати конфіденційність мовлення та ускладнюють незаконний збір аудіоінформації через акустичний канал.

1.5.1 Активний захист інформації

Активний захист мовної інформації від перехоплення спрямованими мікрофонами заснований на принципі створення акустичних перешкод, які унеможливають або значно ускладнюють запис мови[4].

Активний захист можна забезпечити кількома способами:

- Акустичне маскування: генерує шум або мову, щоб заглушити розмовні голоси в приміщенні.
- Акустичні ревербератори: генерують штучну реверберацію, щоб зробити мову нечутною.
- Генератори акустичних вібрацій: генерують вібрації, які спотворюють мову.
- Спрямовані акустичні випромінювачі: генерують звукові хвилі, які заважають роботі спрямованих мікрофонів.

Переваги та недоліки активного захисту

Переваги:

- Ефективний захист від підслуховування спрямованими мікрофонами.
- Легко встановлюється.
- Можна адаптувати до різних умов.

Недоліки:

- Може створювати дискомфорт для присутніх.
- Потребує додаткового обладнання.
- Може бути неефективним з певними типами мікрофонів.

Вибір методу активного захисту може залежити від:

- Розмір і акустика приміщення.
- Кількість людей у приміщенні.

- Рівень загрози.
- Бюджету

Рекомендації щодо вдосконалення активного захисту

- Розробка нових методів акустичних маскування, які роблять мову більш нерозбірливою.
- Використання штучного інтелекту для адаптації звукових перешкод до мови в режимі реального часу.
- Розробка компактних та енергоефективних пристроїв активного захисту.

Пристрої активного захисту використовуються для активного захисту мовної інформації від невиявлених пристроїв несанкціонованого доступу та перехоплення на інших каналах і включають в себе наступні технічні заходи:

1. Пристрої просторового загородження: пристрої просторового загородження: ці пристрої зазвичай використовують генератори шуму в акустичному діапазоні для створення акустичних маскувальних завад. Вони призначені для перешкоджання роботі небажаного приймального обладнання шляхом створення інтенсивного шуму, який заважає правильному прийому аудіосигналів.

2. Віброакустичні пристрої захисту: ці пристрої також використовуються для маскування перешкод і працюють шляхом генерування акустичних коливань, які заважають захопленню і прослуховуванню мовних сигналів.

3. Ультразвукові методи захисту на місці: ці пристрої зазвичай використовуються для захисту від запису мови шляхом генерування високочастотних звуків, які є непомітними для людини, але створюють перешкоди для мікрофонів.

Просторові та прямої видимості завади групуються залежно від того, чи створюють вони акустичні або електромагнітні перешкоди. Ці інструменти можна використовувати окремо або в комбінації для досягнення максимальної ефективності захисту від незаконного збору аудіоінформації[5].

Якщо наперед невідома його робоча частота, то необхідно створити перешкоду

по всьому можливому або доступному діапазону спектру.

Щоб запобігти зняттю інформації спрямованими мікрофонами через акустичний канал, використовуються генератори шуму мовного діапазону, які маскують корисні мовні сигнали і створюють перешкоди. Це досягається за рахунок використання "білого шуму" зі спектральною характеристикою, яка коригується, щоб запобігти отриманню мовної інформації. Для оптимального захисту генератори шуму можуть поєднуватися з комбінованими антенними системами для ефективного покриття різних частотних діапазонів[5].

Основним недоліком використання джерел шуму акустичного діапазону є неможливість комфортно вести переговори. Як показує практика, в приміщенні з ревучим генератором шуму неможливо перебувати більше 10-15 хвилин. Крім того, співрозмовник автоматично захоче кричати на захисний пристрій, знижуючи його ефективність. Тому такі системи використовують для додаткового захисту дверних прорізів, віконних рам, вентиляційних систем тощо.

1.5.2 Пасивний захис інформації

Звукоізоляція - один з найефективніших способів захисту звукової інформації від витоку акустичними шляхами. В її основі лежить зниження рівня звуку, що проходить через стіни, стелю, підлогу та інші конструктивні елементи приміщення.

Звукоізоляція використовується для усунення перехоплення інформації через прямі акустичні шляхи (наприклад, щілини, вікна, двері, вентиляційні отвори) і вібраційні шляхи (наприклад, загороджувальні конструкції, труби водо- і газопостачання, каналізаційні системи)[6].

Принципи звукоізоляції

- Збільшення маси елементів конструкції: чим товща і важча стіна, тим легше вона поглинає звук.
- Використання звукопоглинальних матеріалів: мінеральна вата, пінополіуретан і звукоізоляційні панелі поглинають звукові хвилі і перетворюють їх в тепло.
- Зменшення вібрацій: антивібраційні матеріали та антивібраційні конструкції

зменшують вібрації, що передаються через конструкцію.

- Усунення зазорів і щілин: зазори і щілини в конструкції діють як звукові "мости" і повинні бути закриті.

Переваги звукоізоляції

- Ефективно запобігає витоку звукової інформації.
- Забезпечує приємну акустичну атмосферу в приміщенні.
- Зниження рівня шуму від доріг та сусідів.
- Підвищення енергоефективності будівель.

Недоліки звукоізоляції

- Висока вартість: високоякісні звукоізоляційні матеріали коштують дорого.
- Зменшення корисної площі: товстіші звукоізоляційні матеріали призводять до збільшення товщини стін.

- Складність монтажу: звукоізоляційні матеріали складні в установці і можуть вимагати спеціальних навичок.

Вибір звукоізоляційного матеріалу залежить від:

- рівня шуму, який потрібно звукоізолювати
- Тип стіни, стелі або підлоги
- Вашого бюджету

Рекомендацій щодо звукоізоляції [6]

Зверніться до фахівця зі звукоізоляції, щоб розрахувати необхідний рівень звукоізоляції.

Використовуйте високоякісні звукоізоляційні матеріали відомих виробників.

Переконайтеся, що звукоізоляція встановлена правильно.

Під час проведення звукового ізолювання приміщень, слід урахувати природні звукопоглинальні властивості різних матеріалів.

Матеріал, об'єкт	Густина ρ , кг/м ³	Товщина h , мм	Значення коефіцієнта звукопоглинання α в октавних смугах із середньо геометричними частотами, Гц					
			125	250	500	1000	2000	4000
Алюмінієві перфоровані панелі	20	50	0,15	0,65	1,0	0,99	1,0	1,0
Вініпор напівтвердий	120	50	0,23	0,46	0,93	1,0	1,0	1,0
Деревинно-волокниста плита	–	14	0,032	0,05	0,41	0,57	0,53	–
Залізобетон	–	–	0,01	0,02	0,02	0,02	0,04	0,04
Металеві перфоровані листи	80	60	0,18	0,63	0,9	0,94	1,0	1,0
Міпора	–	60	0,12	0,29	0,55	0,67	0,62	0,85
Пінополістирол	–	15	0,04	0,13	0,18	0,4	–	–
Пінополіуретан	–	50	0,18	0,30	0,74	0,52	–	–
Плити з мінеральної вати	400	20	0,11	0,3	0,85	0,9	0,78	0,73
Шаруватий бетон	–	85	0,63	0,76	0,61	0,65	0,53	–

Рисунок 1.5.1 – Значення коефіцієнта звукопоглинання деяких будівельних матеріалів [4].

Звукоізоляція є ефективним методом захисту мовної інформації від витоку через акустичний канал. Важливо правильно вибрати звукоізоляційні матеріали та виконати монтаж з дотриманням всіх норм і правил.

Також для запобігання пасивному запису мовної інформації в мікрофон через акустичний канал можна використовувати такі методи:

Акустичні бар'єри: розміщення акустичних бар'єрів, таких як шумопоглинаючі матеріали, акустичні панелі або шумозахисні завіси, може зменшити можливість запису мікрофонного мовлення.

Маскування звуку: використання акустичного фону або генераторів шуму, які видають природні звуки, може сплутати мову і ускладнити запис.

Дифузія звуку: використання матеріалів або конструкцій, які розсіюють звук, може ускладнити точне спрямування і запис мови, знижуючи ефективність прослуховування.

Акустичні фільтри: встановлення акустичних фільтрів або пристроїв перешкод, які блокують або приглушують певні частоти, може ускладнити запис мовлення.

Просторова конфігурація: організація та розташування приміщень з

урахуванням акустичної конфіденційності може зменшити ризик збору небажаної інформації.

Важливо правильно розмістити джерело звуку (наприклад, стіл переговорів) в приміщенні.

- Розташовувати джерело звуку подалі від стін, кутів та інших місць, де може утворюватися акустична реверберація.
- Розташовувати джерело звуку так, щоб мікрофон направленої дії знаходився на максимально можливій відстані від нього.
- Використовувати ширми або інші акустичні екрани для того, щоб заблокувати пряму видимість джерела звуку для мікрофона.

Пасивні методи не обов'язково забезпечують такий самий рівень захисту, як активні, але можуть бути ефективним доповненням до загальної системи безпеки.

1.6 Висновки та постановка задач

Отже, у цьому розділі було розглянуто та проаналізовано існуючі методи та засоби захисту інформації від мікрофонного прослуховування, також розглянуто різні акустичні канали витоку інформації, які можуть бути використані для незаконного отримання конфіденційних даних. До кожного з видів каналу витоку інформації було наведено певні технічні характеристики деяких приладів захисту інформації акустичним каналом та порівняно їх між собою.

Акустичні канали витоку інформації які використовують звукові хвилі для передачі або перехоплення інформації.

Віброакустичні канали витоку інформації використовують вібрації твердих поверхонь для передачі звуку.

Електроакустичні канали витоку інформації використовують електричні сигнали для передачі акустичних даних.

Лазерно-акустичні канали витоку інформації використовують лазерний промінь для передачі акустичних сигналів на віддалений об'єкт.

До методів захисту інформації від витоку акустичними каналами включають активні та пасивні методи. Загалом, для ефективного захисту інформації від витоку

акустичними каналами необхідно застосовувати комбіновані методи активного та пасивного захисту, враховуючи специфіку кожного каналу витоку та умови експлуатації захищених приміщень.

Наступні задачі які будуть виконані в ході роботи:

1. Розробка пристрою захисту інформації від перехоплення спрямованими мікрофонами через акустичні канали за рахунок створення генератора шуму.
2. Спроектувати дослідний зразок пристрою.

2. РОЗРОБКА ПРИСТРОЮ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ЗЙОМУ МІКРОФОНОМ НАПРАВЛЕНОЇ ДІЇ

В сучасному світі інформація стає все більш цінним активом. Зростає потреба в захисті конфіденційних переговорів, ділових зустрічей та інших акустичних даних від несанкціонованого зняття. Одним із найпоширеніших методів витоку інформації є використання мікрофонів направленої дії.

2.1 Розробка структурної схеми пристрою

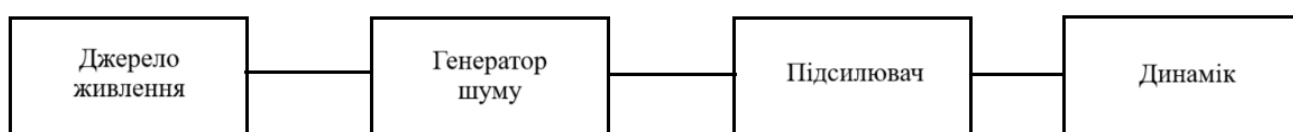


Рисунок 2.1 – структурна схема.

На даній структурній схемі (рис. 2.1) показаний загальний принцип роботи приладу, а саме генератора білого шуму.

Від джерела живлення подається напруга на стабілітрон.

Генератор шуму створює сигнал, який використовуватиметься для створення перешкод.

Вихідний підсилювач посилює перешкоди рівня, достатнього їхнього відтворення через динамік.

Динамік розміщується у приміщенні, яке необхідно захистити від прослуховування.

Докладніше розглянемо кожен блок схеми, в якій використовуються стабілітрон, як вони функціонують і взаємодіють.

Крок 1. Джерело живлення

Джерело живлення забезпечує необхідну постійну напругу для всіх компонентів схеми. Напруга може становити від 9 до 11 В, залежно від обраних компонентів. Важливо, щоб джерело живлення було стабільним і могло забезпечити достатній струм для всіх компонентів схеми.

Крок 2. Генератор шуму на стабілітроні

Стабілітрони можуть використовуватися не тільки для стабілізації напруги, але і для генерації шуму. Стабілітрон, як і стабілітрон KS156A, може генерувати шумовий сигнал в області зворотного пробою. Наприклад, стабілітрон KS156A генерує електричний шум при напрузі 11 В, який може бути використаний для створення акустичних перешкод. Цей шумовий сигнал важливий для забезпечення стабільної роботи генератора шуму та подальшої схеми.

Крок 3. Підсилювач на транзисторі

2SC3198BL цей транзистор використовуються для посилення шумового сигналу, що генерується стабілітроном. транзистор разом з пасивними компонентами (резисторами і конденсаторами) утворює підсилювач, який збільшує рівень шумового сигналу і підходить для створення акустичних перешкод. Посилений шумовий сигнал може бути використаний для різних застосувань, включаючи маскування звуку в приміщенні для захисту конфіденційності розмови.

Крок 4. Динаміки відтворюють генерований шум у навколишньому середовищі, що ускладнює їх прослуховування в приміщенні. Для цієї мети можна використовувати стандартні колонки з імпедансом 8 Ом і потужністю 1-2 Вт.

Основи розроблення захисних пристроїв.

1. Фізичні принципи поширення звукових хвиль

- Звукові хвилі: механічні коливання, що поширюються в середовищі (повітря, вода, тверде тіло).
- Характеристики: частота (Гц), амплітуда (гучність звуку), швидкість поширення (залежить від середовища).
- Відбиття і заломлення: відбиття від поверхонь, заломлення під час переходу з одного середовища в інше (захист конструкціями).
- Вібрація матеріалів: звукові хвилі викликають коливання, які можуть бути сприйняті мікрофонами (наприклад, стіни і вікна).

2. Акустичні канали витоку інформації

- Прямий звуковий канал: безпосередня передача звуку від джерела до приймача (двері, вікна, вентиляційні отвори).

- Віброакустичний канал: звукові хвилі викликають вібрації в конструкції будівлі, які можуть зчитуватися датчиками або стетоскопами.

- Лазерно-акустичний канал: лазерні мікрофони використовують відбите лазерне світло для зчитування вібрацій на поверхнях (наприклад, на віконному склі).

3. Методи виявлення несанкціонованого доступу

- Акустичні датчики: мікрофони або інші датчики контролюють звукове середовище (виявляють підозрілі звуки або аномалії).

- Спектральний аналіз: аналіз спектра звукового сигналу для визначення характеристик мікрофонів та інших підслуховувальних пристроїв.

- Електромагнітне сканування: використання спектрометрів для виявлення електромагнітних випромінювань від прихованого електронного обладнання.

4. Методи перехоплення та захисту

- Генератори білого шуму: генерування фоновому шуму для маскування мовлення та інших звуків, що ускладнює їх виявлення мікрофонами.

- Акустичне екранування: використання звукоізолюючих матеріалів або звукоізолюючих конструкцій для зменшення передачі звукових хвиль через стіни, підлогу, стелю та інші елементи приміщення.

- Генератори вібрації: використання п'єзоелектричних або електромагнітних генераторів для створення вібрацій, що перешкоджають передачі акустичної інформації через конструкцію будівлі.

5. Компоненти захисного пристрою

- Акустичні датчики: датчики, що вловлюють звукові хвилі в приміщенні (ідентифікація потенційних загроз).

- Пристрої, що генерують шум: пристрої, що генерують білий шум або інші акустичні перешкоди для маскування розмов.

- Блок управління: центральний модуль (керує роботою компонентів, обробляє

дані, регулює роботу пристроїв, що генерують шум).

- Система сигналізації: сповіщає про підозрілу поведінку або наявність несанкціонованих підслуховувальних пристроїв.

6. Стандарти та вимоги

- Вимоги до продуктивності: рівень шумозаглушення, чутливість датчиків, надійність системи.
- Регіональні та міжнародні стандарти: ISO/IEC 27001 (інформаційна безпека), галузевий стандарт (захист голосу)[8].

Застосування пристрою

Генератори шуму використовуються для захисту конфіденційної інформації від витоку через акустичні канали.

Генератор шуму встановлюється в приміщенні, де проводяться важливі переговори і наради.

Коли пристрій вмикається під час події, він створює фоновий шум, який заважає прослуховувати розмову.

Він використовується в кабінетах керівників та інших працівників, які мають справу з конфіденційною інформацією.

Його можна встановити на робочому столі або в кутку кімнати для забезпечення максимального охоплення.

Генератор шуму може використовуватися в приміщеннях, де обробляється або зберігається конфіденційна інформація, наприклад, в архіві або серверній кімнаті.

Відстань та умови використання

Відстань:

Для ефективного захисту від підслуховування генератор шуму повинен розташовуватися на відстані не більше 2-5 метрів від джерела конфіденційних розмов.

Якщо приміщення велике, рекомендується використовувати кілька генераторів шуму, які рівномірно розташовані по периметру приміщення або в ключових точках.

Умови:

Генератор шуму повинен працювати за відсутності сильного зовнішнього шуму, який може знизити ефективність.

Діапазон температур обладнання становить від -5°C до 40° .

Вологість: до 80% без конденсації.

Характеристики навколишнього середовища:

Приміщення повинно бути закрито таким чином, щоб рівень шуму не перевищував його і не завдавав дискомфорту оточуючим.

Рекомендується використовувати звукоізоляційні матеріали для оздоблення стін, підлог і стель приміщення. Це підвищує ефективність захисту.

Забезпечує необхідні властивості для захисту

Рівень шуму:

Генератор повинен створювати рівень шуму не менше 80-100 дБ, щоб ефективно блокувати розмову.

Пристрій повинен працювати на частоті від 20 Гц до 20 кГц, що відповідає діапазону чутності людини.

Розміщення:

Генератор слід розміщувати таким чином, щоб він рівномірно покривав всю площу приміщення.

Перед використанням слід відрегулювати гучність і діапазон частот генератора відповідно до умов приміщення.

Отже, можна зробити наступні висноки генератори шуму є ефективним засобом захисту конфіденційної інформації від зйому мікрофоном направленої дії. Правильне розміщення та конфігурація пристрою створюють надійний фоновий шум, який не дозволяє стороннім особам та пристроям чути розмову. Для забезпечення необхідних захисних властивостей важливо враховувати відстань, умови роботи і навколишнє середовище.

2.2 Вибір бази елементів

Для протидії прослуховуванню пропонується використовувати метод генерації

шуму, який заглушає мову та інші звуки, роблячи їх неможливими для розпізнавання мікрофонами.

В якості джерела шуму буде використовуватися стабілітрон KC156A. Стабілітори відомі тим, що вони генерують шум при певному напруженні.

Регулювання шуму

Для регулювання рівня шуму стабілітрона використовується змінний резистор, який слугує дільником напруги.

Підсилення шуму

Оскільки рівень шуму з виходу стабілітрона незначний, його необхідно підсилити. Для цього буде використано підсилювач низької частоти на транзисторі 2SC3198BL, який має високий коефіцієнт підсилення.

Практична реалізація

Під час роботи пристрою з динаміка підсилювача буде чути шум, який заглушатиме мікрофони та підслуховуючі пристрої. Динамік рекомендується встановити біля вікна, стіни або в інших місцях, де може відбуватися прослуховування.

Переваги

- Простота та доступність компонентів
- Ефективність протидії прослуховуванню
- Можливість регулювання рівня шуму

Недоліки

- Необхідність підключення до електромережі
- Можливість виявлення пристрою за шумом

Запропонований метод генерації шуму на основі стабілітрона KC156A є простим, доступним та ефективним способом захисту від прослуховування.

Обґрунтування вибору стабілітрона KC156A для генерації шуму з метою захисту від прослуховування

1. Рівень шуму: стабілітрон KC156A генерує значний рівень шуму при певному напруженні, що робить його ідеальним для даного завдання. В порівнянні з іншими стабілітронами, KC156A має один з найвищих рівнів шуму, що робить його більш

ефективним для заглушення мови та інших звуків.

2. Доступність: KC156A є стабілітроном, який був широко випускався і досі є легко доступним та недорогим. Це робить його економічно вигідним вибором для даного проекту.

3. Надійність: KC156A є надійним компонентом, який має тривалий термін служби та стійкий до перевантажень. Це важливо, оскільки пристрій буде працювати протягом тривалого часу і може піддаватись перепадам напруги.

Всі характеристики стабілітронів було найдено за пошуком[9].

Таблиця 2.1 – порівняння з іншими стабілітронами.

Стабілітрон	Рівень шуму	Ціна	Надійність	Посилання
KC156A	Високий	Низька	Висока	[9]
Д818	Середній	Низька	Висока	[9]
KC1178A	Низький	Низька	Висока	[9]
1N4733A	Низький	Висока	Середня	[9]

Як видно з таблиці, KC156A має найвищий рівень шуму серед представлених стабілітронів, що робить його кращим вибором для даного завдання.

На основі вищезазначених аргументів, KC156A є оптимальним вибором стабілітрона для генерації шуму з метою захисту від прослуховування. Він має високий рівень шуму, доступний, надійний та простий у використанні.

Обґрунтування вибору транзистора 2SC3198BL для підсилювача в генераторі шуму.

2SC3198BL – біполярний транзистор загального призначення NPN-типу[10], який добре підходить для використання в генераторах шуму завдяки своїм наступним характеристикам:

Високий коефіцієнт посилення струму: 2SC3198BL має високий коефіцієнт посилення струму (h_{fe}) до 400, що дозволяє йому ефективно підсилювати низькі рівні шуму, створювані генератором.

Широкий діапазон частот: 2SC3198BL має широкий діапазон частот (до 100 МГц), що дозволяє підсилювати шум у широкому діапазоні частот.

Низький рівень шуму: він має низький рівень шуму, мінімізуючи шум, який додає сам транзистор до шуму, створюваного генератором.

Доступність: 2SC3198BL є доступним і недорогим транзистором, що робить його економічно ефективним вибором для генераторів шуму.

В таблиці 2.2 було наведено порівняльні характеристики різних транзисторів можливих для використання.

Вся інформація про характеристики транзисторів була найдена за посиланням [10].

Таблиця 2.2 – порівняльні характеристики транзисторів

Параметр	2SC3198BL	BC547	2N2222	2N3904
Частотний діапазон (MHz)	До 100	До 100	До 200	До 300
Коефіцієнт посилення (h_{FE})	200-450	110-400	100-300	100-300
Рівень шуму (dB)	1	2	4	4
Максимальна напруга (V)	50	45	40	40
Максимальний струм (A)	0.15	0.1	0.8	0.2
Посилання	[10]	[10]	[10]	[10]

Отже, можна з даної таблиці можна зробити наступні висновки:

Всі розглянуті транзистори мають достатній діапазон частот генератора шуму. 2SC3198BL має краще посилення (200-450) в порівнянні з іншими транзисторасми, що дозволяє краще посилювати сигнали.

2SC3198BL має найнижчий рівень шуму серед розглянутих транзисторів, що вкрай важливо для генератора шуму.

2SC3198BL має достатні характеристики напруги та струму для більшості

застосувань генератора шуму.

Тому транзистор 2SC3198BL є найкращим вибором для генератора шуму завдяки високому посиленню, низькому рівню шуму та відповідним параметрам напруги та струму.

Детальний опис схеми підсилювача на транзисторі 2SC3198BL

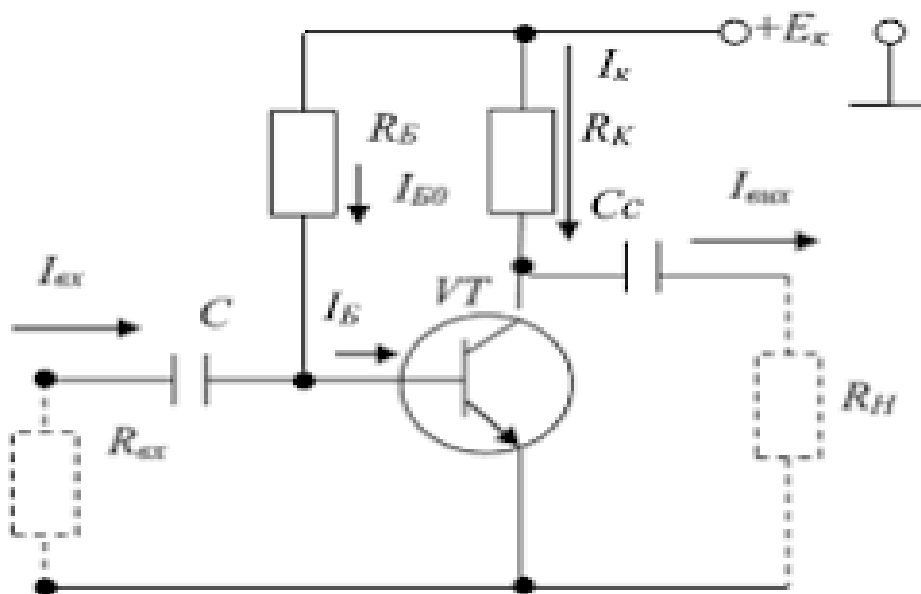


Рисунок 2.2 – схема підсилювача на транзисторі 2SC3198BL[11].

Дана схема підсилювача низької частоти на основі транзистора 2SC3198BL працює наступним чином:

Вхідний сигнал: Напруження шуму з виходу стабілітрона KC156A подається на базу транзистора Q1 через конденсатор C1. C1 блокує постійну складову сигналу, пропускаючи лише змінну складову (шум).

Підсилення: Транзистор Q1 підсилює змінну складову сигналу. Коефіцієнт підсилення транзистора визначається значенням резистора R2. Чим менше значення R2, тим більше буде підсилення.

Вихідний сигнал: Підсилений сигнал з колектора транзистора Q1 подається на динамік.

Саме тому дана схема підсилювача низької частоти на основі транзистора 2SC3198BL є простим та ефективним способом підсилення шуму з виходу стабілітрона KC156A.

2.3 Вибір джерела живлення

Щоб забезпечити автономну роботу розробленого генератора білого шуму, важливо вибрати правильне джерело живлення. Пристрій має бути портативний і повинен працювати без підключення до мережі, тому було вирішено використовувати батарейки як джерело живлення.

Виходячи з цього мають бути наступні вимоги до джерела живлення

Автономність: джерело живлення повинен забезпечувати тривалу роботу пристрою без необхідності його частоті заміни або підзарядки.

Компактний: пристрій повинен бути портативним і простим у використанні, тому джерело живлення не повинно займати багато місця і впливати на простоту використання.

Надійність: джерело живлення має бути надійним і мати постійну напругу протягом усього терміну служби.

Доступність: вибрані джерело живлення повинно бути широко доступне і при необхідності легко заміні.

Тому виходячи з цього можна зробити висновки що саме батарейки є оптимальним варіантом для даного джерела живлення.

Існує кілька типів батарейок, які можна використовувати для живлення генератора білого шуму, а саме:

Лужні батарейки : це найпоширеніший тип батареї. Вони мають високу енергоємність і тривалим терміном служби.

Літієві батарейки: ці батареї мають більш високу щільність енергії і більш тривалий термін служби в порівнянні з лужними батареями.

Заряджальні батарейки: ці батареї можна заряджати повторно, що робить їх екологічно чистими та економічними в довгостроковій перспективі.

Нижче в таблиці 2.3 було показано порівняння різних типів батарейок, що показує їх характеристики для вибору джерела живлення для генератора білого шуму:

Таблиця 2.3 – порівняльні характеристики батарейок[12].

Характеристика	Лужні батарейки	Літієві батарейки	Заряджальні батарейки
Енергетична щільність	Середня	Висока	Висока
Напруга	1,5 В	1,5 В - 3 В (залежно від типу)	1,2 В - 3,7 В (залежно від типу)
Термін служби	Довгий	Дуже довгий	Залежить від кількості циклів заряд-розряд
Стійкість до температур	Середня	Висока	Середня / Висока
Кількість циклів заряд-розряд	Немає	Немає	500-1000+
Вартість	Низька	Середня	Середня/Висока
Доступність	Висока	Середня	Середня
Посилання	[12]	[12]	[12]

Як можна побачити з даної таблиці та враховуючи потреби даного генератора білого шуму, було обрано літієві батарейки як джерело живлення. Це пов'язано з їх помірною енергоемністю, достатньою напругою, тривалим терміном служби, оптимальною вартістю та хорошою доступністю. Вони забезпечують надійну і тривалу автономну роботу пристрою, що має вирішальне значення для його ефективної роботи.

2.4 Висновки до розділу

У розділі було проведено детальний аналіз та розробка структурної схеми пристрою для захисту інформації від зйому мікрофоном спрямованої дії через акустичні канали. На основі розглянутих теоретичних основ, а також практичних вимог до захисту, було здійснено вибір базових елементів, які забезпечать ефективну роботу пристрою.

Також було встановлено теоретичні основи для створення захисних пристроїв та принцип дії, компонентний склад та призначення пристрою.

Створено структурну схему, яка включає всі необхідні компоненти для генерації та підсилення шуму, що ускладнює зйом звукової інформації мікрофонами.

Здійснено вибір стабілітрона, який забезпечує необхідний рівень шуму при певній напрузі, регульованій змінним резистором.

Вибрано попередній підсилювач низької частоти на транзисторі, який має високий коефіцієнт підсилення, що дозволяє значно підвищити рівень шуму на виході стабілітрона.

Визначено місця встановлення динаміків для максимального ефекту заглушення акустичних сигналів в приміщеннях, що захищаються.

Розроблена структурна схема та вибір бази елементів забезпечують створення простого, доступного, ефективного та регульованого пристрою для захисту інформації від перехоплення спрямованими мікрофонами через акустичні канали.

3. МОДЕЛЮВАННЯ РОБОТИ ПРИСТРОЮ

3.1 Обґрунтування вибору елементів пристрою

Як було описано в попередніх розділах для створення даного генератора шуму будуть використовуватися наступні компоненти:

1. Стабілітрон:

Він використовується як джерело шуму.

Стабілітрон KS156A був обраний через його здатність генерувати сильні перешкоди при напрузі близько 11 В.

2. Змінний резистор:

Для того щоб стабілітрон почав генерувати шум, необхідно налаштувати напругу яка подається на нього. Для цього використовується змінний резистор, який виконує функцію дільника напруги. Регулюючи цей резистор, можна обрати оптимальну напругу, при якій стабілітрон генерує максимальний рівень шуму.

3. Транзистор 2sc3198bl:

Рівень шуму, створюваного стабілітроном, невеликий, і для ефективного придушення звуку його необхідно додати. Для цієї мети використовується низькочастотний передпідсилювач.

Був обраний біполярний транзистор 2SC3198BL через його високий коефіцієнт посилення, який може значно збільшити амплітуду шуму.

4. Динамік:

Після посилення шумовий сигнал подається на динамік, який випромінює шум в навколишнє середовище. Динамік встановлюється поблизу вікон, стін або інших місць, де можуть бути встановлені мікрофони направленої дії. В даному випадку буде використано портативну колонку.

5. Додаткові компоненти:

Крім основних компонентів, також будуть використовуватися використовуються інші компоненти, такі як конденсатори та резистори.

Ці компоненти використовуються для стабілізації напруги, фільтрації перешкод, захисту компонентів.

Виходячи з цих даних було складено таблицю 3.1 в якій коротко описано компоненти генератора шуму та їх функції

Таблиця 3.1 – компоненти та їх функції.

Компонент	Функція
Джерело живлення	Забезпечує напругу пристрою
Стабілітрон (KC156A)	Генерація шуму в широкому діапазоні частот
Змінний резистор	Налаштування напруги для стабілітрону
Транзистор (2SC3198BL)	Підсилення шумового сигналу
Додаткові компоненти (конденсатори та резистори)	Стабілізація напруги, фільтрація перешкод, захист компонентів
Динамік	Випромінювання шумового сигналу

Таким чином, генератор білого шуму на стабілітроні використовує комбінацію електронних компонентів для створення, підсилення та випромінювання шуму, що забезпечує ефективний захист від підслуховування.

Також в таблиці 3.2 наведено технічні характеристики даного генератора шуму.

Таблиця 3.2 – технічні характеристики генератора шуму.

Параметр	Значення
Тип транзистора	2SC3198BL
Частотний діапазон генератора	20 – 2000 Гц
Рівень шуму	60 – 110 дБ
Напруга живлення	12 В
Струм споживання	10-15 мА
Коефіцієнт посилення (hFE)	200-450
Рівень власного шуму транзистора	1 дБ
Тип джерела живлення	батарейки

Вихідна напруга	0.5 В
Тип батарейки	літійна
Вихідний сигнал	Сигнал білого шуму
Тип схеми	Підсилювач на NPN транзисторі

Дивлячись на дану таблицю зробимо розрахункові характеристики:

Шумова завіса: з рівнем шуму від 60 до 110 дБ створюється шумова завіса, яка надзвичайно важко проникнути через неї для прослуховування розмови.

Рівномірне розподілення шуму: рівномірний спектральний розподіл білого шуму забезпечує, що жодна частота не переважає, що робить його ефективним у перекритті всіх можливих частот, які можуть містити корисну інформацію.

Високе підсилення: підсилення на рівні 100 дБ гарантує, що навіть слабкі сигнали стають значною частиною загального шумового фону, що забезпечує додатковий захист.

Таблиця 3.3 порівняльні характеристики

Параметр	генератор шуму	Dohm Classic	LectroFan	Adaptive Sound Technologies Sound+Sleep
Частотний діапазон	20 – 2000 Гц	-	20 – 20000 Гц	20 – 20000 Гц
Рівень шуму	60 – 110 дБ	65 дБ	50 – 70 дБ	30 – 85 дБ
Напруга живлення	12 В	120 В	5 В USB	120 В
Струм споживання	10-15 мА	0.2 – 0.3 А	0.5 – 1 А	0.2 – 0.3 А
Тип джерела живлення	Батарейки	Мережа	USB	Мережа
Вихідний сигнал	Сигнал білого шуму	Білий шум	Білий шум, різні звуки природи	Білий шум, природні звуки
Посилання	-	[27]	[28]	[29]

З урахуванням цих характеристик можна вважати, що генератор білого шуму ефективно захищає конфіденційні дані від витоку через акустичні канали, зробивши їх непридатними для прослуховування сторонніми особами або

пристроями.

Отже, ці характеристики забезпечують надійну роботу генератора шуму в широкому діапазоні частот з мінімальними спотвореннями та власним шумом, що робить його ефективним від зйому мікрофоном направленої дії.

3.2 Моделювання роботи підсилювача на транзисторі

Для моделювання схеми було обрано програму Proteus Professional 8 рисунок 3.1.

Proteus 8 Professional – цей пакет являє собою систему схемотехнічного моделювання, засновану на моделі електронних компонентів, прийнятої в Pspice. Відмінною особливістю пакету Proteus Design є можливість моделювання роботи програмованих пристроїв, таких як мікроконтролери, мікропроцесорні системи і DSP[13]. Proteus Design включає в себе більше 6000 електронних компонентів, включаючи всі довідкові дані, а також демонстраційний проект для підвищення кваліфікації.

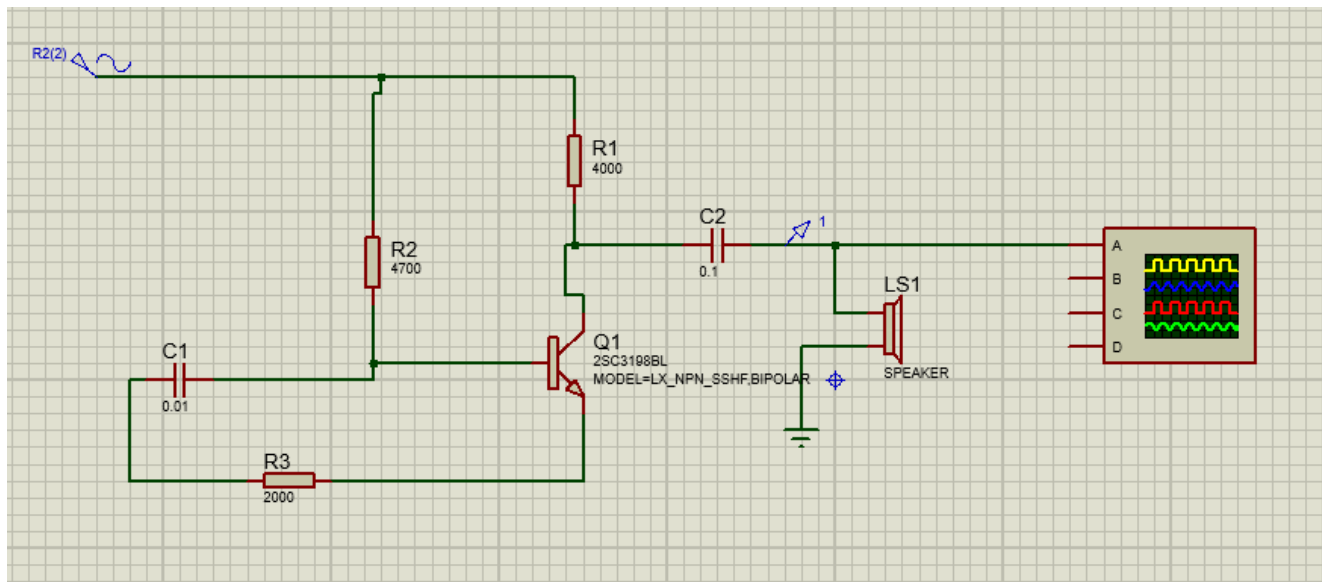


Рисунок 3.1 – схема підсилювача на транзисторі 2SC3198BL в комп'ютерній програмі Proteus 8 Professional.

Відповідно до рисунку 3.1 ця схема представляє собою підсилювач на транзисторі 2SC3198BL, який буде використовуватися для підсилення шумового сигналу, отриманого від генератора білого шуму.

Цей підсилювач працює наступним чином:

1. Вхідний сигнал: сигнал струму (в даному випадку від генератора білого шуму) подається на вхід схеми через конденсатор C1, щоб відсікти постійну складову сигналу і генерувати змінний шум.

2. Базовий струм: резистор R2 генерує базовий струм транзистора Q1 для забезпечення роботи в активному режимі. Він також визначає напругу зміщення бази транзистора.

3. Посилення сигналу: транзистор Q1 підсилює змінний сигнал, що надходить на нього.

4. Колекторний струм: резистор R1 встановлює струм колектора транзистора, тим самим визначаючи його робочу точку і рівень посилення.

5. Стабілізація: резистор R3 і конденсатор C1 стабілізують робочу точку транзистора і покращують лінійність підсилювача.

6. Вихідний сигнал: посилений змінний сигнал з колектора транзистора проходить через конденсатор C2, блокує постійну складову і передаючи змінний сигнал на вихід схеми.

Відповідно до роботи даного підсилювача промодельємо його працездатність та підсилення сигналів.

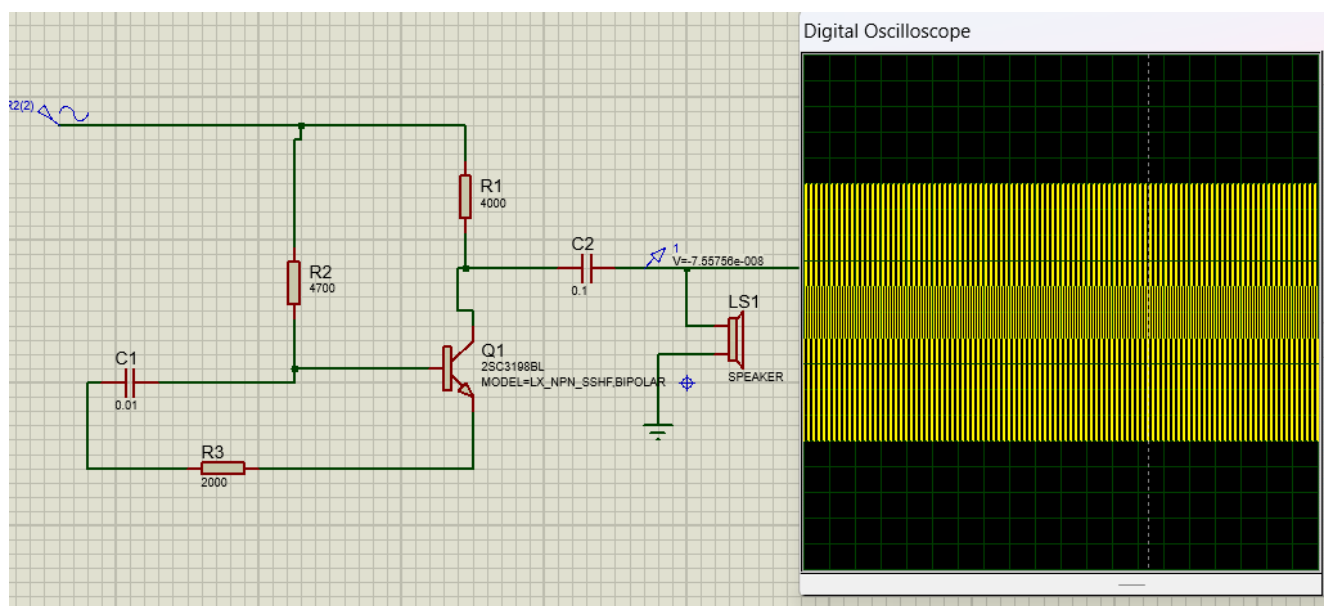


Рисунок 3.2 – показники підсилення на осцилографі.

Як можна побачити з рисунки 3.2 цей осцилограмний графік показує вихідний сигнал підсилювача на транзисторі.

Напруга живлення складає: 11В.

Частота вихідного сигналу: 1 кГц.

Значення напруги на осцилографі складає 0.2 мкВ.

Значення часу знаходяться в діапазоні від 0 до 120.3 мікросекунд.

Значення напруги знаходяться в діапазоні від -1 мкВ до 1 мкВ.

Сигнал має амплітуду близько 2 В, частота сигналу відповідає частоті вхідного сигналу 1 кГц, що вказує на те, що підсилювач правильно підсилює частоту вхідного сигналу без істотних спотворень.

Сигнал має прямокутну форму, що вказує на те, що підсилювач працює в режимі перемикавання, і підсилює вхідний сигнал до рівня, достатнього для забезпечення чітких шумових перешкод.

Аналіз роботи підсилювача показує, що сигнал має достатню амплітуду, що підтверджує ефективну роботу підсилювача. Амплітуда близько 2 В вказує на значне посилення вхідного сигналу. Вихідний сигнал підтримує ту ж частоту, що і вхідний сигнал. Це вказує на те, що підсилювач працює належним чином на цій частоті. Форма сигналу вказує на те, що підсилювач працює в режимі насичення, які використовуються для підсилювачів, що використовуються в схемах генераторів шуму.

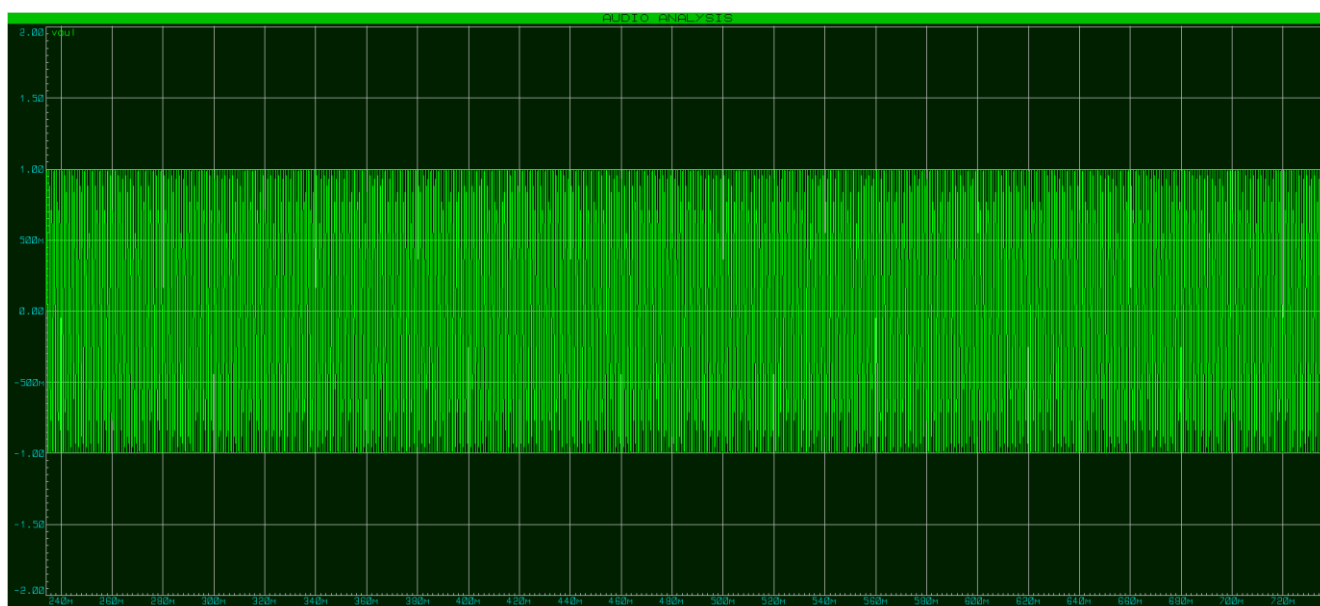


Рисунок 3.3 – аналіз графіку підсилення.

Як видно з рисунку 3.3 можна зробити наступний аналіз:

Аналіз Частотного Спектру Шуму

Частотний спектр шуму на даному графіку складає 1 кГц, він є досить рівномірним у всьому діапазоні частот. Це свідчить про те, що підсилювач буде підсилювати по всьому діапазоні частот рівномірно. Тому білий шум матиме однакове підсилення на всіх частотах.

Частотна залежність інтенсивності шуму: на цьому графіку інтенсивність шуму не є постійною у всьому діапазоні частот. Вона коливається і вказує на наявність піків інтенсивності на різних частотах.

Отже, на графіку ми можемо зробити висновок, що інтенсивність шуму змінюється залежно від частоти і що існують певні частоти з високою інтенсивністю шуму.

На даному графіку інтенсивність шуму коливається приблизно в діапазоні від
Графік показує, що вихідний сигнал підсилювача має випадковий, хаотичний вигляд, який характерний для шуму.

Коефіцієнт посилення підсилювача достатньо високий. Це означає, що він зможе підсилити шум до необхідного рівня.

Лінійність графіка є важливим показником.

На графіку також показано, що підсилювач має однакове посилення в широкому діапазоні частот, оскільки такий сигнал повинен містити всі частоти з однаковою інтенсивністю. Це бажано для генераторів білого шуму.

Отже, можна зробити наступні висновки дана схема транзисторного підсилювача 2SC3198BL ефективно підсилюватиме сигнал змінного шуму, що генерується стабілітроном генератора білого шуму. Завдяки високому підсиленню транзистора ця схема може забезпечити необхідне посилення сигналу на генераторі білого шуму для захисту інформації від зйому мікрофоном направленої дії.

3.3 Моделювання роботи генератора шуму

Для моделювання схеми генератора шуму також було обрано програму Proteus

Professional 8 рисунок 3.4.

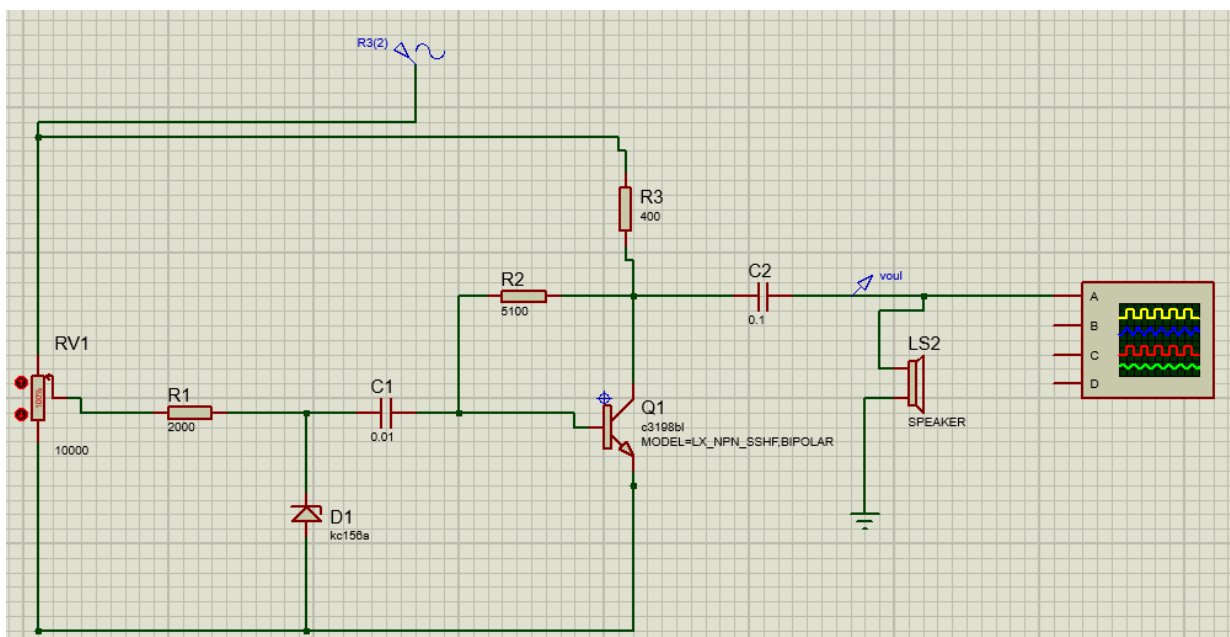


Рисунок 3.4 – схема проектування генератора шуму в комп'ютерній програмі Proteus 8 Professional.

Відповідно до рисунку 3.4 опишемо принцип роботи генератора шуму на основі даного стабілітрона

1. Генерація шуму:

В основі роботи даного генератора лежить принцип використання стабілітрона. Стабілітрон - це напівпровідниковий прилад, який при певному напруженні (напрузі пробую) починає генерувати шум в широкому діапазоні частот.

В даному пристрої використовується стабілітрон KC156A, який при напрузі близько 12 В генерує сильний шум.

Рівень шуму стабілітрона можна регулювати за допомогою змінного резистора. Змінний резистор використовується як дільник напруги, який змінює напругу на стабілітроні, тим самим змінюючи інтенсивність шуму.

2. Підсилення шуму:

Оскільки рівень шуму з виходу стабілітрона незначний, його необхідно підсилити. Для цього використовується попередній підсилювач низької частоти, зібраний на транзисторі 2SC3198BL.

Цей транзистор має високий коефіцієнт підсилення, що дозволяє йому значно

збільшити амплітуду шуму.

3. Виведення шуму:

Підсилений шум подається на динамік, який випромінює його в навколишній простір.

Таким чином, основний принцип роботи генератора білого шуму на стабілітроні полягає у використанні стабілітрона для генерації широкого спектру шумів, діапазон частот шуму включає чутні частоти (20-20000 Гц) і вище. Посилення цього шуму за допомогою передпідсилювача і випромінюванні посиленого сигналу через динамік для створення акустичних перешкод.

Завдяки цьому шум заглушає мікрофони направленої дії, роблячи прослуховування приміщення практично неможливим.

Генератор шуму генерує білий шум, який має рівномірний розподіл енергії в широкому діапазоні частот.

Ефективність роботи генератора шуму залежить від рівня шуму, який він генерує, а також від розташування динаміка.

Переваги:

Простота та доступність компонентів;

Ефективність протидії прослуховуванню;

Можливість регулювання рівня шуму:

Недоліки:

Необхідність підключення до електромережі;

Можливість виявлення пристрою за шумом:

Генератор шуму на основі стабілітрона є простим, доступним та ефективним способом захисту від мікрофонів направленої дії.

Для кращого захисту рекомендується використовувати декілька генераторів шуму, розміщених в різних місцях приміщення.

Також важливо правильно вибрати динамік та його розташування, щоб забезпечити максимальне заглушення мікрофонів.

На рисунку 3.5 показано що генератор шуму працює та створює білий шум завдяки якому злвмисники не зможуть знімати інформацію за допомогою

направленого мікрофона через акустичні канали.

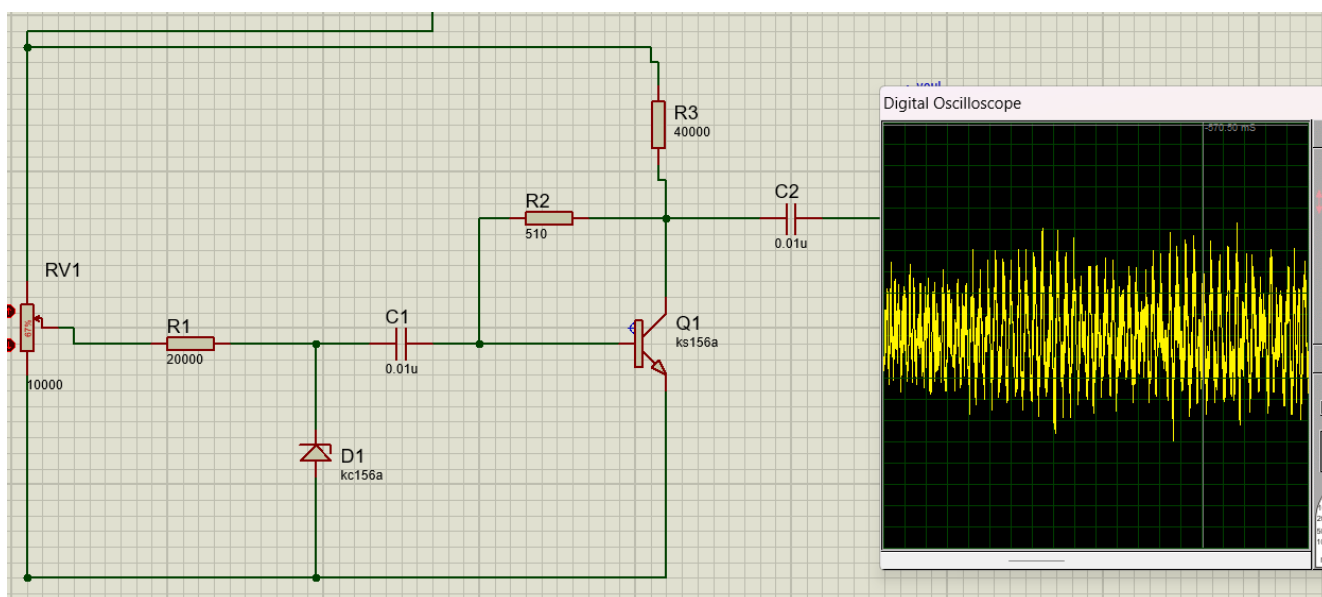


Рисунок 3.5 – графік сигналу.

На цьому графіку показано сигнал, що генерується з генератора шуму і відображається на цифровому осцилографі. З даного графіка можна зробити наступні висновки:

Опис графіка:

Значення напруги на осцилографі складає 0.1 мкВ.

Значення часу знаходяться в діапазоні від 0 до 65.3 мікросекунд.

Значення напруги знаходяться в діапазоні від -0.5 мкВ до 0.5 мкВ.

Форма сигналу є майже синусоїдальним або шумоподібним, з регулярними коливаннями в діапазоні напруг. Ці коливання здаються випадковими, що відповідає характеристикам білого шуму.

Характеристики сигналу

Частота сигналу на даному рисунку становить 1к Hz. Як можна бачити з сигналу це високочастотний шумовий сигнал.

Регулярні коливання сигналу вказують на те, що він є шумовим. Це підтверджується випадковим характером коливань амплітуди.

Отже, сигнал є високочастотним шумом, що підтверджується його коливальним характером і амплітудою. Цей тип сигналу є типовим для генераторів білого шуму, які використовуються для маскування акустичної інформації від

направлених мікрофонів.

З урахуванням випадкових коливань і широкого діапазону частот, цей сигнал буде ефективним для маскування розмов або інших акустичних сигналів, перешкоджаючи їх перехопленню мікрофонами або іншими засобами прослуховування.

Цей аналіз підтверджує, що сигнал, який ми бачимо на осцилограмі, відповідає характеристикам білого шуму і може бути ефективно використаний для захисту приміщень від прослуховування.

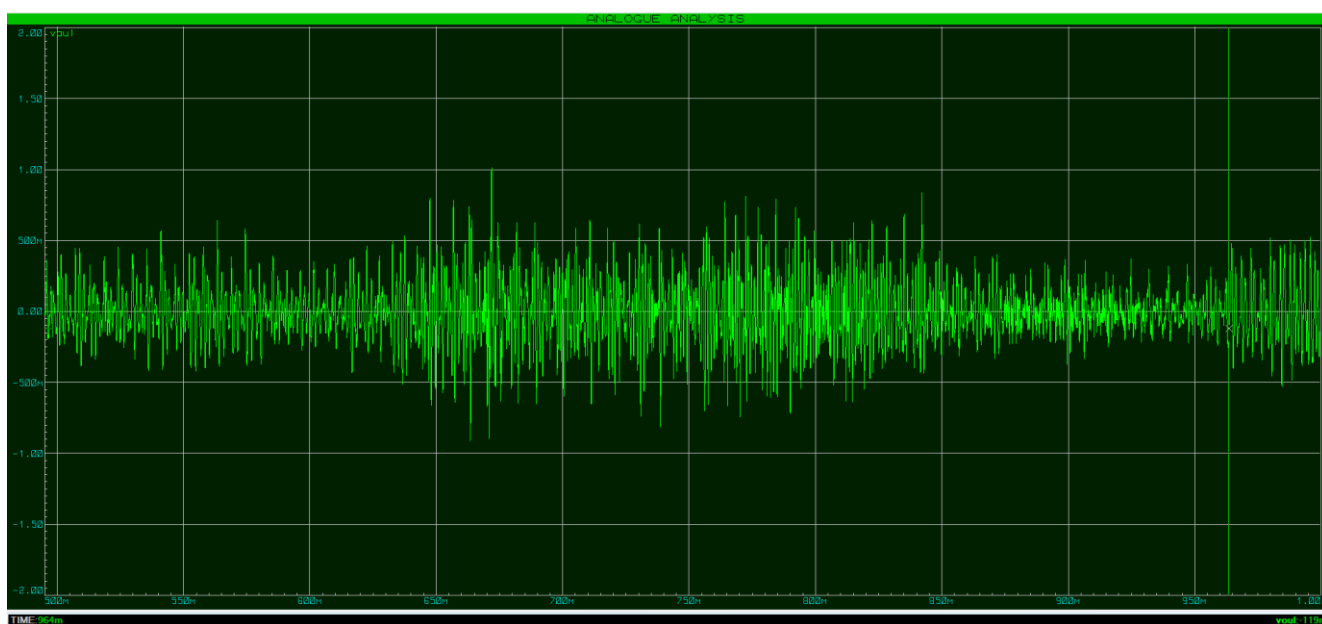


Рисунок 3.6 – графік сигналу.

На цьому графіку (рисунок 3.6) показана тимчасова діаграма сигналу, отриманого за допомогою аналізу. На графіку показано зміну амплітуди сигналу з часом.

Напруга з джерела 12 В.

Частота сигналу 1 мГц.

Амплітуда сигналу варіюється в межах від приблизно -2.0 В до 2.0 В, що показує досить широкий діапазон значень.

З даного графіка можна зробити наступні висновки:

Графік показує, що сигнал є випадковим і не має помітної періодичності, що є типовою ознакою шумового сигналу. Ця форма хвилі часто використовується для

маскування акустичної інформації.

Амплітуда сигналу рівномірно розподіляється між позитивними і негативними значеннями, що вказує на те, що сигнал не має постійної складової (складової постійного струму) дека.

Випадковість сигналу: сигнал має випадковий характер, що відповідає генератору білого шуму. Такі сигнали ефективно використовуються для маскування звукової інформації, оскільки звукову інформацію важко відфільтрувати або розпізнати.

Ефективність маскування: через випадковий характер сигналу він може ефективно маскувати мову та інші акустичні сигнали та запобігати їх перехопленню мікрофонами та іншими пристроями підслуховування.

Шумові характеристики: якщо графік не містить періодичних компонентів або значних піків, з цього можна зробити висновок, що цей сигнал насправді є шумом і призначений для створення акустичних перешкод.

Ось кілька ключових моментів, які можна виділити з цього графіка:

Діапазон частот: графік охоплює частоти від 20 Гц до 2 кГц, що вказує на те, що генератор шуму працює в широкому діапазоні частот.

Спектральна однорідність: на графіку не видно великих піків або провалів, і шум може бути рівномірно розподілений по всьому частотному діапазону.

Аналіз амплітудної характеристики: відсутність значних коливань амплітуди сигналу вказує на те, що генератор шуму має досить стабільну амплітудну характеристику у всьому частотному спектрі.

Відсутність гармонік: на графіку не показано наявності гармонік або інших форм спотворень, що є позитивним показником якості генератора шуму.

Виходячи з цього аналізу, можна сказати, що генератор шуму забезпечує рівномірний і стабільний вихід у широкому діапазоні частот і є бажаною характеристикою для генератора шуму, особливо в додатках, де потрібен широкий діапазон частот шумового сигналу.

Отже, такий сигнал можна використовувати з генератором білого шуму, щоб захистити кімнату від прослуховування. Це відповідає меті даної роботи, а саме

розробка пристрою захисту інформації від зйому мікрофоном направленої дії акустичним каналом.

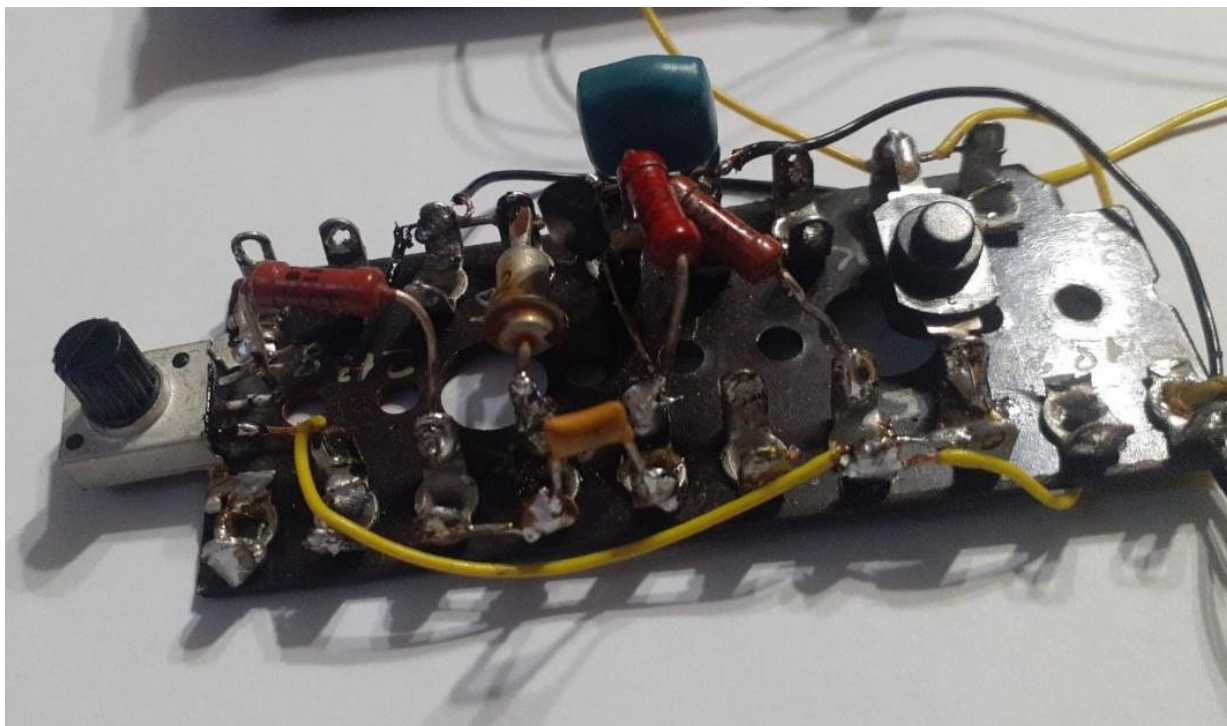


Рисунок 3.7 – розроблений пристрій

За даною схемою було розроблено дослідницький зразок генератора білого шуму для захисту інформації від зйому мікрофоном направленої дії.

3.4 Висновки до розділу

У даному розділі дипломної роботи було проведено обґрунтування вибору елементів пристрою і моделювання роботи генератора шуму. Зокрема, цей розділ включав дві важливі частини: обґрунтування вибору компонентів та моделювання генератора шуму. Було спроектовано та проаналізовано дослідний зразок пристрою, також описано принцип роботи пристрою, схему його побудови, а також процес моделювання його роботи в програмі Proteus.

Моделювання роботи генератора шуму в Proteus показує, що пристрій генерує білий шум у широкому діапазоні частот. Рівень шуму можна регулювати за допомогою змінного резистора.

Обґрунтування вибору елементів підтвердило, що використані компоненти є оптимальними для досягнення цілей проекту, а саме створення надійного пристрою

для захисту від акустичного перехоплення направленим мікрофоном.

Також було виконано спектральний аналіз сигналу за допомогою осцилографа, отриманого від генератора шуму. Форма сигналу показує, що сигнал схожий на шум із випадковими коливаннями, що відповідає характеристикам білого шуму.

Ефективність шумозаглушення: виміряні параметри шуму, такі як амплітуда і діапазон частот, дозволяють ефективно маскувати аудіосигнал і запобігати його перехоплення мікрофоном.

Форма сигналу показує стабільний високочастотний шум і підходить для маскувння акустичних сигналів в широкому діапазоні частот.

ВИСНОВКИ

В ході роботи були досліджені різні канали витоку акустичної інформації. Особливу увагу було приділено каналам витоку акустичної інформації, віброакустичним каналам, лазерним каналам та електроакустичним каналам витоку інформації. Також були розглянуті методи захисту інформації від витоку, включаючи методи активного та пасивного захисту.

Було встановлено, що активні методи захисту включають використання генераторів білого шуму та інших засобів, що створюють шумові перешкоди, тоді як пасивні методи спрямовані на покращення звукоізоляції та використання спеціальних матеріалів.

Також була розроблена структурна схема пристрою і підібрана елементна база, необхідна для його реалізації. Аналіз і порівняння технічних характеристик існуючих пристроїв дозволили визначити оптимальні компоненти для створення ефективної системи захисту.

Також було обґрунтовано вибір елементів пристрою та проведено моделювання його роботи. Результати моделювання показують, що обраний підхід і компоненти забезпечують надійний захист при прослуховуванні через спрямовані мікрофони. Ефективність шумових перешкод, що генеруються в широкому діапазоні частот, була підтверджена аналізом спектра сигналу білого шуму.

Саме тому генератор шуму на основі стабілітрона є простим, доступним та ефективним способом захисту від прослуховування.

Пристрій генерує білий шум в широкому діапазоні частот, що робить його ефективним проти різних типів мікрофонів та підслуховуючих пристроїв.

Рівень шуму можна регулювати, що дозволяє адаптувати пристрій до конкретних умов.

Отже, виконана робота досягла поставленої мети: розробка пристрою для захисту інформації від перехоплення спрямованими мікрофонами через акустичні канали за рахунок генератора білого шуму. Реалізований генератор білого шуму є ефективним засобом для створення шуму, що ускладнюють зйом інформації.

Перелік посилань

1. Іванченко С. О. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: навчальний посібник\ Іванченко С. О. – Київ: КПІ, 2016. Ст. 44-55
2. Бібліотека / ТЗІ / ЗАГАЛЬНИЙ ОГЛЯД СИСТЕМ ВІБРОАКУСТИЧНОГО ЗАШУМЛЕННЯ – м. Київ 2009.
3. Бібліотека / ТЗІ / ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ – м. Київ 2009.
4. Методи та засоби захисту від шуму: навчальний посібник \ Чернігів: НУЧП, 2016.
5. Калюжний О. Е. ДОСЛІДЖЕННЯ ШЛЯХІВ ПРОТИДІЇ ЗАСТОСУВАННЮ ЗАСОБІВ МОБІЛЬНОГО ЗВ'ЯЗКУ ВІД НЕСАНКЦІОНОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ / Калюжний О. Е Київ – 2022, с.8-40
6. Маскування звуку [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/Sound_masking
7. РОЇК О. М., МІРОНОВА Ю. В., ВОЛКОТРУБ О. П. ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ АКУСТИЧНИМИ КАНАЛАМИ / РОЇК О. М., МІРОНОВА Ю. В., ВОЛКОТРУБ О. П., “ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ” – № 1 – 2015 с. 50-53
8. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT) - 2023
9. Радіокомпоненти \ Радіокомпоненти активні \ Стабілітрони \ Стабілітрони вітчизняні \ Стабілітрон 2С156А (=КC156А)
<https://radiokomponent.com.ua/ua/product/stabilitron-2s156a-ks156a/>
10. Космодром. Біполярні транзистори. [Електронний ресурс]. – Режим доступу <https://www.kosmodrom.ua/tranzistor-bipolyarnyy/2sc3198.html>
11. Ковалишин Б.М. / Підсилювачі електричних сигналів. Робоча програма / Київ – 2018 ст. 9-11

12. Е-Katalog. Батарейки і акумулятори: типи, форми та розміри [Електронний ресурс]. – Режим доступу <https://ek.ua/ua/post/3519/325-batareyki-i-akkumulyatory-tipy-formy-i-razmery/>
13. Proteus 8 Professional [Електронний ресурс]. – Режим доступу : <https://dnipro.lvivservice.com.ua/vstanovlennya-proteus-8-professional>
14. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г., Чуприн В.М., Горбунов О.О. - Захист інформації в телекомунікаційних системах. Київ – 2009. ст. 223 – 235
15. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г., Чуприн В.М., Горбунов О.О. - Захист інформації в телекомунікаційних системах. Київ – 2009. ст. 223 - 235
16. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г., Чуприн В.М., Горбунов О.О. - Захист інформації в телекомунікаційних системах. Київ – 2009. ст. 223 - 235
17. Yogasleep Dohm UNO White Noise Sound Machine (White) With Real Fan Inside for Non-Looping White Noise, For Travel, Office Privacy, Meditation, Sleep Aid For Adults & Baby, Registry Gift [Електронний ресурс]. – Режим доступу : <https://www.amazon.com/Marpac-Machine-Non-Looping-Privacy-Therapy/dp/B07DJL3Y8K>
18. Sound Masking System, Sound Machines [Електронний ресурс]. – Режим доступу : <https://www.pureresonanceaudio.com/products/sound-masking-system-featuring-12-ceiling-speakers-white-noise-sound-masking-generator>
19. Speech Privacy System, Yamaha VSP-1 [Електронний ресурс]. – Режим доступу : <https://www.cinenow.fr/produits/4754-yamaha-ysp-1>
20. Noise Masking Generator, Cambridge Sound Management 1 [Електронний ресурс]. – Режим доступу : <https://www.proacousticsusa.com/cambridge-qt-100-sound-masking-generator.html>
21. Катаєв В. С., Яремчук Ю. Є. Метод активного захисту інформації від зняття лазерними системами акустичної розвідки // Захист інформації. — 2019. — Т. 21, № 1. — Ст. 34—39.

22. Катаєв В. С., Яремчук Ю. Є. Метод активного захисту інформації від зняття лазерними системами акустичної розвідки // Захист інформації. — 2019. — Т. 21, № 1. — Ст. 34—39.

23. Катаєв В. С., Яремчук Ю. Є. Метод активного захисту інформації від зняття лазерними системами акустичної розвідки // Захист інформації. — 2019. — Т. 21, № 1. — Ст. 34—39.

24. Логвін Є. О., Степаненко В. М. ЗАХИСТ АКУСТИЧНОЇ ІНФОРМАЦІЇ ВІД ДИСТАНЦІЙНОГО ПЕРЕХОПЛЕННЯ ОПТИЧНИМИ ЗАСОБАМИ ТЕХНІЧНОЇ РОЗВІДКИ. Навчально-науковий Фізико-технічний інститут. 2023. Ст. 136-139.

25. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г., Чуприн В.М., Горбунов О.О.. Захист інформації в телекомунікаційних системах. – Київ - 2009 ст. 58-75.

26. AN-G-2000 Acoustic Noise Generator [Електронний ресурс]. – Режим доступу : <https://www.spyshopeurope.com/en/ang-2200-acoustic-noise-generator/1155/195>

27. Yogasleep Dohm Classic (White) The Original White Noise Sound Machine, Soothing Natural Sounds from a Real Fan, Sleep Therapy for Adults & Baby, Noise Cancelling for Office Privacy & Meditation/ [Електронний ресурс]. – Режим доступу : <https://www.amazon.com/Marpac-Classic-Original-White-Machine/dp/B00HD0ELFK?th=1>

28. Adaptive Sound Technologies LectroFan High Fidelity White Noise Machine with 20 Unique Non-Looping Fan and White Noise Sounds and Sleep Timer [Електронний ресурс]. – Режим доступу : <https://www.amazon.com/LectroFan-White-Noise-Machine-Non-Looping/dp/B00JU8P8VY?th=1>

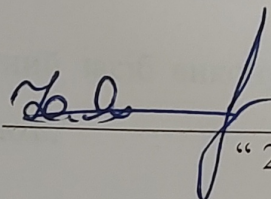
29. Sound+Sleep SE Special Edition High Fidelity Sleep Sound Machine with Real Non-Looping Nature Sounds, Fan Sounds, White/Silver [Електронний ресурс]. – Режим доступу : <https://www.amazon.com/Sound-Fidelity-Non-Looping-Adaptive-Technology/dp/B01LY3BP8G?th=1>

Додаток А. Технічне завдання

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ

Голова секції “Управління інформаційною
безпекою” кафедри МБІС
д.т.н., професор

 Юрій ЯРЕМЧУК
“ 22 ” березня 2024 р.

ТЕХНІЧНЕ ЗАВДАННЯ

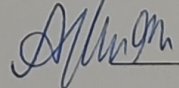
до бакалаврської дипломної роботи на тему:

“Розробка пристрою захисту інформації від зйому мікрофоном направленої дії
акустичним каналом”

08-72.БДР.020.00.066 ТЗ

Керівник бакалаврської дипломної роботи

к.т.н., доцент каф. МБІС

 Шиян А. А.

“ ”

Вінниця – 2024 р.

1. Найменування та область застосування

Програмний засіб методу захисту від атаки типу прослуховування. Область застосування: захист інформаційних ресурсів від несанкціонованого доступу акустичним каналом.

2. Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ № 80 від 11.03.2024 р.

3. Мета та призначення розробки

3.1 Мета розробки: розробка ефективного методу захисту від зйому мікрофоном направленої дії.

3.2 Призначення: розроблений програмний засіб виконує захист від зйому мікрофоном направленої дії акустичним каналом.

4. Джерела розробки

4.1. Ахрамович В. М. Ідентифікація й аутентифікація, керування доступом // Сучасний захист інформації. – 2016. №4. – С. 47-51.

4.2. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л.Бурячок, Р.В.Гришук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

4.3. Єсін В.І. Безпека інформаційних систем і технологій / В.І.Єсін, О.О. Кузнецов, Л.С. Сорока. – Харків: ХНУ імені В.Н. Каразіна, 2013. – 632 с.

4.4. ZakariaOmar, ZangooeiToomaj, MohdAfiziMohdShukran. Enhancing Mixing Recognition-Based and Recall-Based Approach in Graphical Password Scheme. IJACT, Vol. 4, No. 15, pp. 189-197, 2012.

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.2 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків;

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок

5.2.3 Програмний засіб повинен виконувати свої функції.

6. Вимоги до програмної документації

6.1 Обов'язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.4

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист розроблюваного програмного засобу від несанкціонованого використання.

7.2 Неможливість отримання доступу незареєстрованих користувачів до інформаційних ресурсів.

8. Техніко-економічні показники

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу.

9. Стадії та етапи розробки

№ з/п	Назва етапів бакалаврської дипломної роботи	Початок	Закінчення
1.	Визначення напрямку бакалаврської роботи, формулювання теми	21.03.2024	22.03.2024
2.	Аналіз предметної області обраної теми	01.04.2024	07.04.2024
3.	Розробка алгоритму роботи	08.04.2024	29.04.2024
4.	Написання бакалаврської роботи на основі розробленої теми	09.05.2024	19.05.2024
5.	Передзахист бакалаврської дипломної роботи	20.05.2024	24.05.2024
6.	Виправлення, уточнення, корегування бакалаврської дипломної роботи	25.05.2024	09.06.2024
7.	Захист бакалаврської дипломної роботи	12.06.2024	17.06.2024

10. Порядок контролю та прийому

10.1 До приймання бакалаврської дипломної роботи надається:

– ПЗ до бакалаврської дипломної роботи;

- демонстрація результату бакалаврської дипломної роботи;
- презентація;
- відзив керівника роботи;
- відзив рецензента

Технічне завдання до виконання прийняв Усач Усач М. В.

Додаток Б. Ілюстраційний матеріал

Розробка пристрою захисту інформації від зйому мікрофоном направленої дії акустичним каналом

Виконав студент групи 2KITC20-Б Усач Микола Васильович

Науковий керівник: к.т.н., доцент каф. МБІС Шиян А. А.

Актуальність теми

Акустичні канали є одним з найуразливіших шляхів витоку інформації. Звукові коливання можуть передаватися через стіни, вікна, вентиляційні системи та інші конструкційні елементи будівель, що робить можливим несанкціонований зйом інформації. Це створює серйозну загрозу для безпеки конфіденційних даних.

Мета роботи

Мета даної роботи - розробити пристрій для захисту інформації від перехоплення спрямованими мікрофонами через акустичний канал.

Для досягнення мети роботи необхідно вирішити наступні завдання

1. Проаналізувати методи та засоби для захисту інформації від зйому мікрофоном направленої дії акустичним каналом.
2. Спроекувати ефективний пристрій, що забезпечує захист від перехоплення акустичної інформації.
3. Розробити дослідний зразок пристрою.

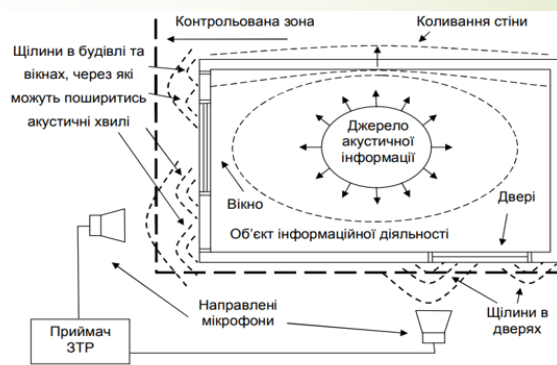
Об'єктом дослідження є акустичний канал витоку інформації та методи його захисту від зняття мікрофоном.

Предметом дослідження є пристрій захисту інформації від зняття мікрофоном направленої дії акустичним каналом.

Практична цінність цієї роботи полягає у створенні пристрою захисту інформації від зйому мікрофоном направленої дії акустичним каналом для забезпечення конфіденційності мовлення та запобігання несанкціонованому доступу до критично важливої інформації

Теоретичні основи

Акустичні канали витоку інформації утворюється шляхом перехоплення мовних сигналів об'єкта інформаційної діяльності акустичними мікрофонами направленої дії чи акустичними антенатами захобів технічної розвідки що встановлюються за межами контрольованої зони в зоні прямої видимості з вікон чи інших отворів



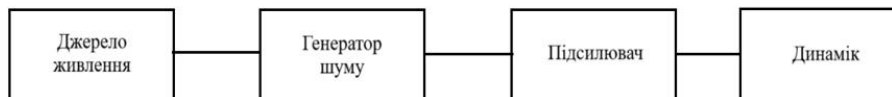
Принцип дії захисних пристроїв

В основі роботи захисних пристроїв лежить генерація шуму, що маскує корисний сигнал і робить його невлотимим для мікрофонів. Основні компоненти таких пристроїв включають генератори шуму, підсилювачі та випромінювачі шуму.



Розробка структурної схеми

На цьому етапі було створено структурну схему пристрою, яка включає всі необхідні компоненти для генерації та підсилення шуму. Розроблено блок-схему, яка дозволяє чітко уявити взаємодію між різними частинами пристрою.



Компонентний склад пристрою

Пристрій складається з наступних основних компонентів:

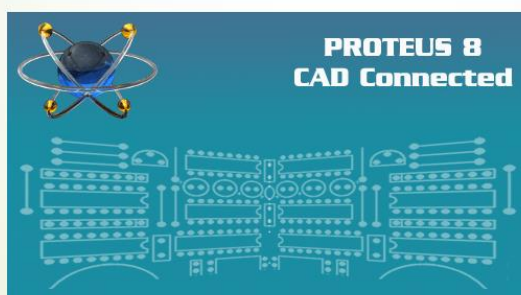
- Джерело живлення.
- Змінний резистор: для регулювання напруги на стабілітрон
- Стабілітрон KC156A старого зразку, який генерує шумовий сигнал.
- Підсилювач на транзисторі 2SC3198BL, який підсилює рівень шуму.
- Динамік, який встановлюється у місцях можливого перехоплення інформації, таких як вікна, стіни та вентиляційні отвори.
- Додаткові компоненти: конденсатори та резистори.

Принцип дії пристрою

Компонент	Функція
Джерело живлення	Забезпечує напругу пристрою
Змінний резистор	<u>Налаштування напруги для стабілітрону</u>
<u>Стабілітрон (KC156A)</u>	<u>Генерація шуму</u>
<u>Підсилювач на транзисторі (2SC3198BL)</u>	Підсилення шумового сигналу
Додаткові компоненти (конденсатори та резистори)	Стабілізація напруги, фільтрація перешкод, захист компонентів
Динамік	<u>Випромінювання шумового сигналу</u>

Засіб моделювання пристрою

Proteus 8 Professional – цей пакет являє собою систему схемотехнічного моделювання, засновану на моделі електронних компонентів, прийнятої в Pspice. Професійна електроніка є стандартом для багатьох компаній, і Proteus 8 Professional є одним з найбільш ефективних та потужних інструментів для розробки електронних пристроїв.



Моделювання роботи підсилювача

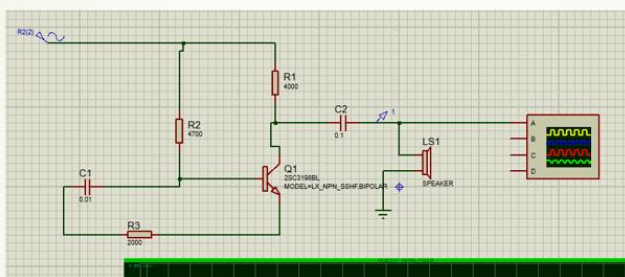
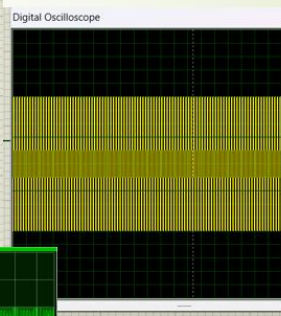
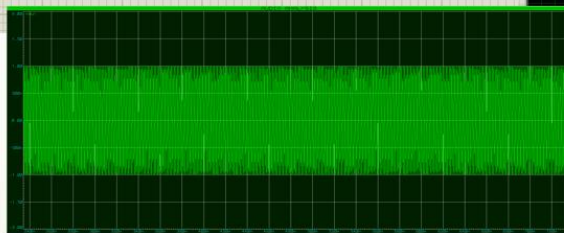


Схема підсилювача



Показники осцилографа



Аналіз графік підсилення

Моделювання генератора шуму

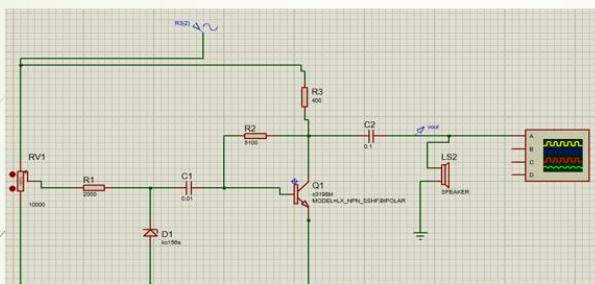
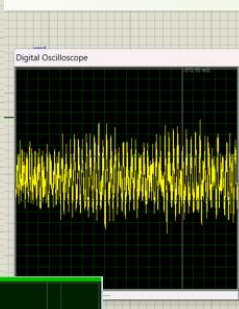
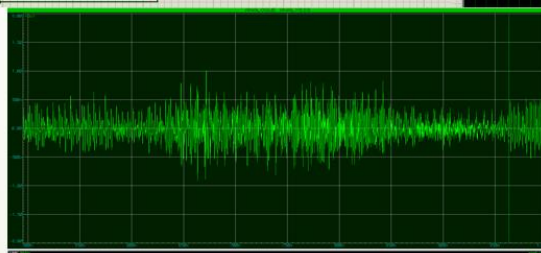


Схема генератора шуму

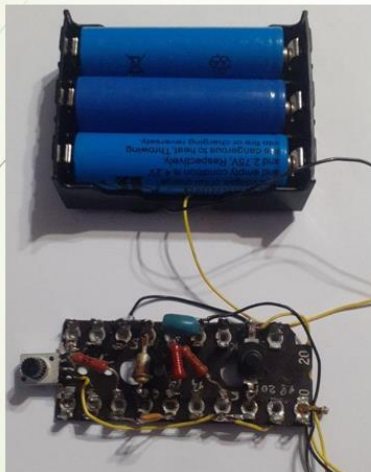


Показники осцилографа



Графік сигналу пристрою

Розроблений дослідницький зразок генератора білого шуму



Висновки

В результаті виконаної роботи були досліджені канали витоку акустичної інформації.

Також була розроблена структурна схема пристрою і підібрана елементна база, необхідна для його реалізації.

Здійснено моделювання роботи пристрою.

Було розроблено ефективний пристрій для захисту інформації від зйому мікрофоном спрямованої дії через акустичні канали. Пристрій забезпечує надійний захист конфіденційних даних завдяки генерації та підсиленню шумового сигналу, що заважає перехопленню інформації.

Дякую за увагу !

Додаток В. Протокол перевірки на антиплагіат

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Розробка пристрою захисту інформації від зйому мікрофоном
направленої дії акустичним каналом

Тип роботи: бакалаврська дипломна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unichesk

Оригінальність 91 %

Схожість 9 %

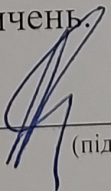
Аналіз звіту подібності (відмітити потрібне):

1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

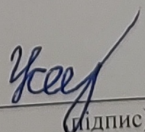
Особа, відповідальна за перевірку


(підпис)

Коваль Н.П.
(прізвище, ініціали)

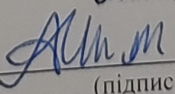
Ознайомлені з повним звітом подібності, який був згенерований системою Unichesk щодо роботи.

Автор роботи


(підпис)

Усач М.В.
(прізвище, ініціали)

Керівник роботи


(підпис)

Шиян А.А.
(прізвище, ініціали)