

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Захист мовної інформації в контрольованому приміщенні з урахуванням
акустичних властивостей приміщення»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

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

Виконав: здобувач вищої освіти групи СЗДМ 61
Кирило РАУС

Керівник: Юрій ПЕПА _____.
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2026

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

Кафедра Технічних систем кіберзахисту

Ступінь вищої освіти магістр

Спеціальність Кібербезпека та захист інформації

Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ

Завідувач кафедри ТСК

_____ Олександр ТУРОВСЬКИЙ

«___» _____ 2025 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Раусу Кирилу Ігоровичу

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:

«Захист мовної інформації в контрольованому приміщенні з урахуванням акустичних властивостей приміщення»

Керівник кваліфікаційної роботи Юрій ПЕПА

(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 20.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи:

Методи та засоби захисту мовної інформації

Акустичні властивості приміщень та їх вплив на поширення мовного сигналу

Моделі оцінки ефективності захисту мовної інформації в контрольованих приміщеннях

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз загроз та особливостей приміщення для захисту мовної інформації

2. Моделювання поширення мовного сигналу та оцінка ефективності захисту

3. Розробка та технічна оцінка заходів захисту мовної інформації

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах

6. Дата видачі завдання 30.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

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

Здобувач вищої освіти

(підпис)

Кирило РАУС

(Ім'я, ПРИЗВИЩЕ)

Керівник роботи

(підпис)

Юрій ПЕПА

(Ім'я, ПРИЗВИЩЕ)

РЕФЕРАТ

Текстова частина бакалаврської (магістерської) кваліфікаційної роботи: 80 стор., 5 табл., 29 джерел.

Метою кваліфікаційної роботи є розробка та дослідження комплексу методів, алгоритмів і технічних рішень для підвищення рівня конфіденційності мовної інформації в конкретному контрольованому приміщенні шляхом використання або нейтралізації його акустичних властивостей. Відтак, об'єктом дослідження є процеси та засоби захисту мовної інформації в контрольованих приміщеннях з урахуванням акустичних властивостей середовища.

Предмет дослідження – процеси та закономірності розповсюдження мовного сигналу і його перетворення в інформаційних каналах витоку, а також методи, алгоритми та засоби протидії цим процесам.

У роботі проаналізовано міжнародні стандарти з інформаційної безпеки, методи оцінювання загроз, методи оцінювання порушників, ефективність методів оцінювання, вплив оцінювання на процес створення систем захисту інформації, фактори, що впливають на оцінювання загроз та порушників, рекомендації та стратегії вдосконалення процесу оцінювання.

Галузь використання – технічний захист інформації, зокрема, забезпечення конфіденційності мовних переговорів. Конкретно, знання та рішення, розроблені в рамках цієї теми, застосовуються у сфері створення та експлуатації контрольованих приміщень (зон), де обробляється конфіденційна інформація (державна таємниця, комерційна таємниця, службова інформація).

Апробація:

Р.О. Чечко, К.І. Раус, ОЦІНКА ЕФЕКТИВНОСТІ БІОМЕТРИЧНИХ СИСТЕМ .
Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.53-54. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: захист мовної інформації, акустичні властивості приміщення, контрольоване приміщення, активні методи захисту, пасивні методи захисту, маскування мовного сигналу, оцінка ефективності захисту, акустичне моделювання.

ABSTRACT

Text section of the Bachelor's (Master's) qualification work: 80 pages, 5 tables, 29 sources.

The aim of the qualification work is the development and study of a set of methods, algorithms, and technical solutions to enhance the confidentiality of speech information in a specific controlled room by utilizing or neutralizing its acoustic properties. Consequently, *the object of the research* is the processes and means of protecting speech information in controlled rooms, taking into account the acoustic properties of the environment.

The subject of the research is the processes and patterns of speech signal propagation and its transformation in information leakage channels, as well as the methods, algorithms, and tools for countering these processes.

The work analyzes international standards on information security, threat assessment methods, intruder assessment methods, the effectiveness of evaluation methods, the impact of assessment on the process of designing information protection systems, factors affecting threat and intruder assessment, and recommendations and strategies for improving the evaluation process.

Field of application – technical information protection, in particular ensuring the confidentiality of verbal communications. Specifically, the knowledge and solutions developed within this topic are applied in the creation and operation of controlled rooms (zones) where confidential information is processed (state secrets, trade secrets, official information).

Keywords: speech information protection, acoustic properties of a room, controlled room, active protection methods, passive protection methods, speech signal masking, protection effectiveness assessment, acoustic modeling.

ЗМІСТ

	Стор.
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	7
ВСТУП.....	8
Розділ 1 ЗАГАЛЬНІ ПІДХОДИ ДО ПОБУДОВИ СИСТЕМИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В КОНТРОЛЬОВАНОМУ ПРИМІЩЕННІ	11
1.1 Аналіз акустичних властивостей приміщення.....	11
1.2. Визначення каналів витоку мовної інформації.....	15
1.3. Технічні засоби захисту мовної інформації	18
1.4. Організаційні та режимні заходи.....	21
1.5 Комплексний підхід до інтеграції системи	24
Розділ 2 АНАЛІЗ АКУСТИЧНИХ ВЛАСТИВОСТЕЙ КОНТРОЛЬОВАНОГО ПРИМІЩЕННЯ ТА ЗАГРОЗ ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ.....	30
2.1. Фізичні основи поширення звуку у приміщеннях	30
2.2 Акустичні параметри контрольованого приміщення.....	35
2.3 Оцінка рівня загроз для конкретного приміщення.....	40
2.4 Висновки	45
Розділ 3 МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В КОНТРОЛЬОВАНОМУ ПРИМІЩЕННІ	48
3.1. Пасивні методи захисту мовної інформації.....	48
3.2. Активні методи захисту мовної інформації.....	53
3.3 Організаційні методи захисту мовної інформації	58
3.4 Висновки	60
4.1. Опис контрольованого приміщення та умов експлуатації.....	64
4.2 Аналіз потенційних каналів витоку мовної інформації в контрольованому приміщенні.....	66
4.3 Вибір та обґрунтування комплексу технічних засобів захисту мовної інформації	68
4.4 Оцінка ефективності запропонованої системи захисту мовної інформації	70
4.5 Аналіз результатів та практичні рекомендації щодо підвищення рівня захисту мовної інформації	72
ВИСНОВКИ.....	75
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	78

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

- T3I – Технічний захист інформації
- RT60 – Час ревербації

ВСТУП

Актуальність дослідження. Необхідність підвищення ефективності технічного захисту конфіденційних переговорів в умовах постійно зростаючих загроз інформаційній безпеці. Сучасні, високочутливі засоби акустичної та віброакустичної розвідки здатні перехоплювати мовну інформацію через різноманітні канали витоку, а цінність цієї інформації в політичній, військовій та комерційній сферах неухильно зростає. Недостатній або неточний облік індивідуальних акустичних властивостей контрольованих приміщень (звукоізоляція огорожувальних конструкцій, внутрішня реверберація) призводить до того, що існуючі системи захисту часто виявляються неефективними або потребують неоптимальних витрат. Таким чином, розробка науково обґрунтованих, адаптованих та економічно доцільних методів захисту, що враховують реальну акустичну картину приміщення, є ключовим завданням для гарантування конфіденційності та національної безпеки.

Наукова новизна дослідження полягає в розробці та обґрунтуванні удосконаленої фізико-математичної моделі поширення маскованого мовного сигналу, яка комплексно враховує як зовнішню звукоізоляцію, так і внутрішні ревербераційні характеристики приміщення, що дозволяє створити нові критерії оптимізації параметрів систем активного зашумлення, націлених на мінімізацію енергоспоживання при гарантованому зниженні розбірливості мови за межами контрольованої зони, а також в обґрунтуванні методики акустичного паспортування для оперативного виявлення критичних шляхів витоку. Практичне значення отриманих результатів полягає у можливості їх використання для розробки методичних рекомендацій та нормативних документів з атестації та проектування контрольованих приміщень, а також для створення спеціалізованого програмного забезпечення, яке дозволить інженерам-захисникам прогнозувати та налаштовувати ефективність систем акустичного та віброакустичного захисту, забезпечуючи гарантований рівень конфіденційності при обробці критично важливої інформації.

Об'єкт дослідження – Процес захисту мовної інформації в приміщенні.

Предмет дослідження – Процеси поширення мовного сигналу та методи їхньої нейтралізації з урахуванням акустики приміщення.

Мета роботи – Розробити комплекс рішень для ефективного захисту мовної інформації з урахуванням акустичних властивостей приміщення.

Наукові завдання:

- проаналізувати існуючі методи та засоби захисту мовної інформації в контрольованих приміщеннях;
- дослідити акустичні властивості приміщень та їх вплив на поширення мовного сигналу і ризики витоку інформації;
- розробити фізико-математичну модель поширення маскованого мовного сигналу з урахуванням зовнішньої звукоізоляції та внутрішньої реверберації приміщення;
- створити методику оцінки ефективності активних і пасивних заходів захисту мовної інформації в реальних умовах експлуатації приміщень;
- обґрунтувати підходи до акустичного паспортування приміщень для оперативного виявлення критичних шляхів витоку та оптимізації систем захисту.

Методи дослідження – аналіз документів і літератури, порівняльний аналіз, ризик-аналіз, кейс-стаді.

Практичне значення одержаних результатів полягає у можливості їх безпосереднього використання під час організації комплексного захисту мовної інформації в контрольованих приміщеннях, де існує ризик її витоку через акустичні канали. У межах дослідження здійснено оцінювання акустичних властивостей приміщення, моделювання поширення звукових хвиль та визначення чинників, що впливають на рівень захищеності, що дозволяє формувати обґрунтовані технічні рішення щодо підвищення ефективності захисту інформації.

Отримані результати можуть бути використані під час проєктування або модернізації приміщень для проведення конфіденційних переговорів з урахуванням їх реальних акустичних характеристик, таких як реверберація та звукопоглинання. Запропоновані підходи забезпечують коректний вибір звукопоглинальних і звукоізоляційних матеріалів, що мінімізує рівень передавання

мовного сигналу за межі контрольованої зони та зменшує ризики його перехоплення.

Практична цінність результатів проявляється також у можливості їх застосування для оцінювання загроз витоку інформації через будівельні конструкції, вентиляційні канали та інженерні комунікації. На основі проведених розрахунків визначено можливість ефективного впровадження засобів активного та пасивного акустичного маскування, які враховують спектральні характеристики мовного сигналу та параметри конкретного приміщення.

Розроблені рекомендації можуть бути покладені в основу методики аудиту захищеності приміщень, що може застосовуватися у державних, комерційних та інших структурах, які працюють з конфіденційною інформацією. Крім того, отримані результати створюють передумови для розроблення спеціалізованого програмного забезпечення з моделювання акустичних процесів та автоматизованого вибору оптимальних засобів технічного захисту.

Запропоновані заходи дозволяють істотно підвищити рівень інформаційної безпеки об'єкта, забезпечити відповідність сучасним вимогам і стандартам технічного захисту мовної інформації та зменшити ймовірність її перехоплення через акустичні канали.

Розділ 1

ЗАГАЛЬНІ ПІДХОДИ ДО ПОБУДОВИ СИСТЕМИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В КОНТРОЛЬОВАНОМУ ПРИМІЩЕННІ

Захист мовної інформації — діяльність, спрямована на запобігання витоку інформації, яка циркулює у вигляді акустичних хвиль (голосу людини). Якщо інформація існує у вигляді акустичних хвиль, які створюються за допомогою голосового апарату людини, вона називається мовною [1].

1.1 Аналіз акустичних властивостей приміщення

Всі, крім матеріального каналу витоку відносяться до т.з. технічних каналів витоку інформації. При цьому, технічні канали витоку інформації можуть бути як природними так й штучними (спеціально створеними зловмисниками). Відповідно до ДСТУ 3396.2-97 (Захист інформації. Технічний захист інформації. Терміни та визначення) [2].

Аналіз акустичних властивостей приміщення є фундаментальним етапом побудови системи захисту мовної інформації, оскільки рівень поширення звукового сигналу та можливі шляхи витоку безпосередньо залежать від фізичних параметрів середовища. Основними складовими такого аналізу є геометричні характеристики приміщення, матеріали конструкцій та обробки, ревербераційні властивості, а також моделювання поширення мовного сигналу.

Акустичні канали витоку інформації формуються внаслідок поширення звукових хвиль у повітрі через відкриті двері, вікна й інші вентиляційні отвори [3]. Форма, обсяг і розміри приміщення визначають розподіл акустичної енергії та створюють потенційні зони концентрації мовного сигналу. Прямокутні приміщення з паралельними стінами формують стоячі хвилі, які концентрують звук у певних ділянках, що збільшує ризик витоку інформації. Наявність колон, ніш, виступів або інших архітектурних елементів може сприяти розсіюванню звуку, зменшуючи його інтенсивність у певних напрямках. Проте такі елементи можуть створювати непередбачувані траєкторії поширення хвиль, особливо у зоні вентиляційних каналів або дверних прорізів, що потребує додаткового

моделювання.

Обсяг і висота приміщення визначають швидкість загасання звуку та інтенсивність його відбиттів. У великих приміщеннях звукова енергія розподіляється більш рівномірно, що знижує локальну концентрацію сигналу, однак тривалий час реверберації може підвищувати ризик перехоплення інформації на відстані. У малих приміщеннях високий акустичний тиск у локальних зонах збільшує інтенсивність сигналу біля стін і вентиляційних отворів.

Акустичні властивості поверхонь приміщення визначаються їх коефіцієнтами звукопоглинання. Тверді гладкі матеріали, такі як бетон, скло або плитка, відбивають більшість звукових хвиль, що збільшує кількість відбиттів і тривалість реверберації. М'які матеріали, такі як килими, штори, акустичні панелі або спеціальні облицювальні матеріали, поглинають звукову енергію, знижуючи інтенсивність сигналу і мінімізуючи його витік за межі приміщення. Для забезпечення ефективного захисту мовної інформації необхідно поєднувати матеріали з різними характеристиками поглинання для різних частотних діапазонів людської мови.

Час реверберації (RT60) є критично важливим показником, що визначає тривалість затухання звуку після припинення джерела сигналу. Приміщення з довгим RT60 створює додаткові проблеми для захисту мовної інформації, оскільки мовний сигнал зберігає розбірливість навіть після того, як його основна частина вже припинилася. Оптимальне значення RT60 для приміщень, де проводяться конфіденційні переговори, зазвичай знаходиться у межах 0,4–0,6 секунди для низьких та середніх частот, що дозволяє забезпечити достатню розбірливість мовлення всередині приміщення і одночасно зменшити його витік.

Комп'ютерне моделювання дозволяє передбачити, як мовний сигнал поширюватиметься у приміщенні та за його межами. Використання акустичних моделей допомагає визначити траєкторії хвиль, локальні концентрації звуку, зони посилення або загасання сигналу. Моделювання враховує геометрію приміщення, розташування меблів, матеріали поверхонь та вентиляційні канали. На основі таких даних можна оптимально розташувати акустичні панелі, меблі та технічні засоби

маскування мовного сигналу, щоб знизити рівень потенційного витоку.

Результати детального аналізу акустичних властивостей приміщення дозволяють ідентифікувати слабкі місця для витоку інформації та визначити необхідні технічні та організаційні заходи. Це включає вибір матеріалів з високими коефіцієнтами поглинання, оптимізацію розташування меблів, застосування перегородок та акустичних бар'єрів, а також інтеграцію активних систем маскування сигналу. Такий підхід забезпечує зменшення ймовірності перехоплення мовної інформації через акустичні канали та підвищує загальний рівень захисту приміщення.

Аналіз акустичних властивостей приміщення також передбачає оцінку спектрального складу мовного сигналу та рівнів шуму в приміщенні. Мовна інформація характеризується частотним діапазоном приблизно 300–3400 Гц, при цьому деякі голосові інтонації та консонанти можуть мати більш високі частоти. Важливо враховувати взаємодію цього спектру з акустичними властивостями матеріалів та конструкцій, оскільки відбивальні та поглинаючі характеристики поверхонь залежать від частоти. Наприклад, тверді поверхні добре відбивають низькочастотні сигнали, а м'які матеріали більш ефективно поглинають високі частоти. Тому для захисту мовної інформації доцільно комбінувати матеріали з різними акустичними властивостями, створюючи багат шарові конструкції або застосовуючи дифузори та звукопоглинаючі панелі, що оптимально знижують енергію сигналу в зоні потенційного витоку.

Особливу увагу слід приділити вентиляційним системам, дверним і віконним прорізам, а також щілинам у конструкціях приміщення. Ці елементи часто виступають критичними каналами витоку звуку. Дослідження показують, що навіть при використанні високоякісних звукопоглинаючих матеріалів у стінах і стелі, звукові хвилі можуть просочуватися через вентиляційні решітки або непродумані дверні ущільнення. Для таких зон застосовуються спеціальні шумозахисні решітки, гнучкі звукопоглинаючі вставки та активні системи компенсації шуму, що генерують маскувальний сигнал протилежної фази для зменшення розбірливості мовлення поза приміщенням.

Важливою складовою є оцінка часу затухання звуку для різних частотних діапазонів. Для цього застосовуються стандартні методи вимірювання RT60, а також спектральний аналіз затухання сигналу за допомогою спеціалізованого програмного забезпечення. Отримані дані дозволяють визначити, в яких ділянках приміщення концентрація акустичної енергії може бути найбільшою і, відповідно, які місця потребують додаткового захисту. Наприклад, кути приміщення та зони біля стін часто характеризуються локальним посиленням сигналу, що підвищує ризик його перехоплення.

Моделювання поширення мовного сигналу у приміщенні включає використання методів геометричної акустики, таких як метод променів, метод зображень або скінченних елементів, що дозволяє визначити траєкторії відбиття та інтенсивність сигналу в будь-якій точці. При цьому враховується не лише конфігурація приміщення та розташування джерел шуму, але й зміни акустичного середовища під час експлуатації — рух меблів, присутність людей, відкриття дверей. Таке моделювання дозволяє прогнозувати ефективність як пасивних, так і активних заходів захисту, включаючи розташування шумопоглинаючих панелей, маскувальних джерел та акустичних екранів.

Активні методи захисту мовної інформації, зокрема системи генерації шуму або «білий шум», повинні бути інтегровані з урахуванням реальної акустики приміщення. При цьому параметри шуму (інтенсивність, спектр, напрямок поширення) підбираються так, щоб забезпечити мінімальний вплив на внутрішнє середовище та роботу персоналу, одночасно знижуючи розбірливість мовлення за межами контрольованої зони. Оптимізація таких систем передбачає визначення критичних частот, які найбільш впливають на розбірливість мови, та регулювання параметрів генератора шуму для максимального ефекту при мінімальних енергетичних витратах.

Пасивні методи, такі як звукопоглинаючі панелі, акустичні завіси, перегородки та облицювальні матеріали з різними коефіцієнтами поглинання, дозволяють значно знизити рівень витоку звуку. Важливою практичною задачею є вибір оптимального поєднання матеріалів для різних частотних діапазонів, що

дозволяє забезпечити ефективність захисту без зайвих витрат. Також доцільно застосовувати дифузори та конструктивні елементи, які розсіюють звукову енергію, зменшуючи концентрацію сигналу в певних зонах.

Комплексний аналіз акустичних властивостей приміщення включає також розробку методики акустичного паспортування. Така методика передбачає систематичне вимірювання параметрів приміщення, складання карти інтенсивності мовного сигналу та визначення критичних зон. Акустичний паспорт дозволяє оперативно ідентифікувати слабкі місця, коригувати параметри активних та пасивних систем захисту і проводити регулярний контроль ефективності заходів.

В результаті, детальний аналіз акустичних властивостей приміщення є необхідною передумовою для побудови системи захисту мовної інформації. Він дозволяє комплексно врахувати геометрію приміщення, матеріали конструкцій, внутрішню реверберацію та шляхи потенційного витоку, що забезпечує ефективне поєднання активних та пасивних заходів захисту. Використання сучасних методів моделювання та акустичного паспортування дозволяє підвищити надійність системи, мінімізувати ризики перехоплення мовної інформації та забезпечити економічно обґрунтоване застосування технічних засобів.

1.2. Визначення каналів витоку мовної інформації

Визначення каналів витоку мовної інформації є ключовим етапом побудови системи захисту, оскільки саме через ці канали конфіденційний мовний сигнал може потрапити за межі контрольованого приміщення і стати доступним для несанкціонованого перехоплення. Витоки інформації можуть відбуватися через конструктивні елементи приміщення, інженерні системи та технічні канали перехоплення. Комплексний підхід до їх виявлення дозволяє ідентифікувати потенційні ризики і впровадити ефективні технічні та організаційні заходи.

До конструктивних каналів витоку належать стіни, перекриття, стелі, підлога, двері та вікна. Стіни з низькою звукоізоляцією або тонкі перегородки створюють можливість передачі мовного сигналу через тверді конструкції, особливо у високочастотному діапазоні. Дверні прорізи та ущільнення навколо них

є одними з найвразливіших місць, через які звук може передаватися за межі приміщення. Скляні поверхні та великі вікна, особливо тонкі склопакети, сприяють швидкому поширенню високочастотних компонентів мовного сигналу. Для зниження витоків необхідно застосовувати багатошарові або звукопоглинаючі конструкції, спеціальні ущільнювачі для дверей та вікон, а також додаткові бар'єри у вигляді перегородок або акустичних панелей.

Вентиляційні канали, шахти інженерних комунікацій, електропроводка, водопровідні труби та інші інженерні системи можуть виконувати функцію акустичних каналів, передаючи звукову енергію на великі відстані. Звукові хвилі можуть поширюватися вздовж трубопроводів і вентиляційних каналів, що створює додаткові ризики витоку інформації за межі приміщення. Особливо уразливими є вентиляційні решітки, через які звук може виходити у суміжні приміщення або коридори. Для мінімізації таких витоків застосовуються акустичні демпфери, шумоглушники, спеціальні вигини каналів та звукопоглинаючі вставки.

Крім конструктивних та інженерних шляхів, існують технічні канали перехоплення, що використовуються для незаконного або несанкціонованого запису мовної інформації. До них належать мікрофони, віброакустичні датчики, бездротові перехоплювачі, мобільні пристрої, комп'ютери та інші електронні засоби. Навіть незначні вібрації, передані через стіни або меблі, можуть бути використані для відновлення мовного сигналу спеціалізованими технічними засобами. Усунення або контроль таких каналів включає фізичне блокування сигналу, використання екранувальних матеріалів, спеціальні технічні засоби активного маскування та регламентацію використання електроніки в контрольованих приміщеннях.

Для комплексної оцінки каналів витоку застосовуються експериментальні та розрахункові методи. Експериментально визначають рівні звукового тиску у різних точках приміщення та суміжних зонах, виявляють потенційно уразливі місця та перевіряють ефективність існуючих заходів ізоляції. Розрахункові методи включають моделювання поширення звукових хвиль із врахуванням геометрії приміщення, матеріалів поверхонь та конфігурації інженерних систем. На основі

отриманих даних формується план посилення звукоізоляції, встановлення акустичних бар'єрів та інтеграція технічних засобів маскування мовного сигналу.

Окрему увагу під час визначення каналів витоку мовної інформації слід приділяти умовам експлуатації контрольованого приміщення. Рівень заповненості приміщення, наявність меблів, розташування робочих місць, а також характер проведених у ньому заходів безпосередньо впливають на інтенсивність поширення мовного сигналу. Наприклад, порожні приміщення з твердими поверхнями мають підвищений рівень відбиття звукових хвиль, що може призводити до збільшення ефективної дальності їх поширення через конструктивні та інженерні канали.

Важливим фактором є також частотний склад мовного сигналу. Низькочастотні компоненти мають здатність поширюватися через масивні конструкції та інженерні елементи на значні відстані з меншими втратами, тоді як високочастотні складові легше проходять через щілини, отвори та тонкі перегородки. Тому під час аналізу каналів витоку необхідно враховувати спектральні характеристики мовної інформації та особливості матеріалів, з яких виконані елементи приміщення.

Окрему групу ризиків становлять так звані комбіновані канали витоку, що поєднують акустичні та електромагнітні механізми передачі інформації. До них належать випадки, коли мовний сигнал перетворюється у вібрації або електричні коливання в елементах інженерних мереж чи технічних пристроях, після чого може бути знятий дистанційно. Такі канали є особливо небезпечними, оскільки їх складно виявити без спеціальних засобів контролю та вимірювальної апаратури.

У процесі визначення каналів витоку доцільно проводити зонування території навколо контрольованого приміщення. Виділяються зони можливого прийому мовної інформації, включаючи суміжні приміщення, коридори, технічні поверхи та зовнішні ділянки будівлі. Аналіз кожної зони дозволяє оцінити реальний рівень загрози та встановити пріоритетність захисних заходів залежно від критичності інформації, що обробляється або обговорюється.

Практика показує, що ефективно визначення каналів витоку мовної інформації неможливе без регулярного контролю та повторної оцінки стану

захищеності приміщення. Зміна конфігурації інженерних систем, ремонтні роботи, встановлення нового обладнання або зміна сценаріїв використання приміщення можуть призвести до появи нових каналів витоку або підвищення ефективності вже існуючих. Тому система аналізу повинна бути динамічною та адаптивною.

Узагальнюючи, процес визначення каналів витоку мовної інформації є багатоетапним завданням, що поєднує технічний аналіз, акустичні вимірювання та оцінку експлуатаційних факторів. Його результати формують основу для вибору адекватних методів захисту та дозволяють забезпечити необхідний рівень конфіденційності мовної інформації в контрольованому приміщенні.

Таким чином, детальний аналіз каналів витоку мовної інформації дозволяє ідентифікувати всі потенційні шляхи передачі сигналу за межі контрольованого приміщення та розробити комплексні заходи для їх нейтралізації. Це забезпечує високий рівень безпеки конфіденційної інформації та є ключовою умовою побудови ефективної системи захисту мовної інформації.

1.3. Технічні засоби захисту мовної інформації

Технічні засоби захисту мовної інформації є основою системи безпеки контрольованого приміщення, оскільки саме вони забезпечують нейтралізацію ризиків витоку інформації через конструктивні, інженерні та технічні канали.

До пасивних заходів відносяться звукопоглинальні та звукоізоляційні матеріали, багатошарові перегородки, двері з ущільненнями та акустичні панелі, які знижують інтенсивність звукових хвиль і запобігають передачі мовного сигналу за межі приміщення. Особливу увагу приділяють вибору матеріалів з високим коефіцієнтом поглинання у частотному діапазоні людської мови від 300 Гц до 3 кГц, оскільки саме ці частоти несуть найбільшу інформаційну складову. Розташування меблів, перегородок та акустичних бар'єрів змінює траєкторії поширення звуку, створюючи додаткові перешкоди для витоку інформації.

Активні засоби включають системи маскування мовної інформації, генератори шуму та віброакустичні установки, які створюють контрольовані акустичні або вібраційні перешкоди, роблячи мовний сигнал нерозбірливим для

сторонніх. Системи маскування мовного сигналу генерують акустичний фон у спектрі мовлення, що перекриває мовні компоненти і не впливає на комфорт людей у приміщенні.

Віброакустичні засоби створюють коливання поверхонь конструкцій, унеможливаючи точне відтворення сигналу зовнішніми пристроями. Інтеграція пасивних і активних методів дозволяє досягти комплексного захисного ефекту, при якому багатошарові перегородки та акустичні панелі в поєднанні з генераторами шуму забезпечують значне зниження інтенсивності сигналу у всіх потенційних каналах витоку. При проектуванні системи захисту враховуються частотні характеристики мовного сигналу, геометрія приміщення, наявність інженерних і конструктивних каналів витоку, а також комфорт людей у приміщенні під час використання активних систем. Такий підхід дозволяє створити контрольоване акустичне середовище, забезпечити високий рівень безпеки та значно знизити ймовірність перехоплення мовної інформації сторонніми особами.

Окрім базових пасивних та активних засобів, у системі захисту мовної інформації широко застосовуються спеціалізовані технічні пристрої, спрямовані на зменшення ймовірності перехоплення сигналу через суміжні приміщення та інженерні мережі. До таких засобів належать акустичні екрани, локальні звукопоглинальні конструкції та спеціальні облицювальні матеріали, що встановлюються у найбільш уразливих зонах приміщення. Їх використання дозволяє локалізувати мовний сигнал у межах робочої зони та зменшити рівень акустичного поля поблизу потенційних каналів витоку.

Важливу роль відіграють технічні засоби захисту вентиляційних та інженерних каналів. Для цього застосовуються акустичні лабіринти, шумоглушники та демпфувальні вставки, які встановлюються у вентиляційних шахтах і повітропроводах. Такі елементи значно знижують рівень поширення мовного сигналу вздовж інженерних систем, не порушуючи при цьому їх функціональне призначення. Особливої ефективності досягають комбіновані рішення, де пасивні звукопоглинальні матеріали доповнюються активними віброакустичними засобами.

Окрему категорію становлять технічні засоби захисту від несанкціонованого електронного перехоплення. До них належать пристрої контролю та обмеження використання електронних засобів у контрольованому приміщенні, а також системи виявлення активних і пасивних технічних засобів розвідки. Вони дозволяють своєчасно ідентифікувати наявність прихованих мікрофонів, радіопередавачів або інших пристроїв зняття інформації, що можуть використовуватися для перехоплення мовного сигналу.

Значну увагу під час впровадження технічних засобів захисту приділяють їх узгодженню з архітектурними та конструктивними особливостями приміщення. Неправильно підібрані або некоректно встановлені засоби можуть не лише знизити ефективність захисту, але й створити нові канали витоку. Тому проектування системи захисту мовної інформації здійснюється з урахуванням акустичних характеристик приміщення, коефіцієнтів звукопоглинання поверхонь, ревербераційних властивостей та особливостей розміщення інженерних комунікацій.

Важливим етапом є оцінка ефективності технічних засобів захисту мовної інформації. Для цього застосовуються методи акустичних вимірювань, що дозволяють визначити рівень звукового тиску у контрольованому приміщенні та за його межами, а також коефіцієнти ослаблення мовного сигналу у потенційних каналах витоку. Результати вимірювань використовуються для коригування параметрів активних систем, оптимізації розташування пасивних елементів та підвищення загального рівня захищеності.

Не менш важливим аспектом є експлуатація технічних засобів захисту мовної інформації. Активні системи маскування потребують регулярного контролю працездатності, перевірки спектральних характеристик шуму та корекції рівнів сигналу відповідно до змін умов у приміщенні. Пасивні елементи, у свою чергу, повинні зберігати свої акустичні властивості протягом усього терміну експлуатації, що потребує періодичного огляду та, за необхідності, заміни або модернізації.

Окремо слід зазначити роль автоматизованих систем управління захистом мовної інформації. Такі системи забезпечують централізований контроль активних

засобів, дозволяють адаптувати параметри маскування залежно від часу доби, типу заходів або кількості людей у приміщенні. Це підвищує ефективність захисту та зменшує негативний вплив активних систем на акустичний комфорт персоналу.

Узагальнюючи, технічні засоби захисту мовної інформації є багаторівневою системою, що поєднує пасивні, активні та організаційно-технічні рішення. Їх правильний вибір, інтеграція та експлуатація дозволяють створити надійний бар'єр на шляху витоку мовної інформації та забезпечити відповідний рівень конфіденційності в контрольованому приміщенні. Комплексне застосування таких засобів є необхідною умовою побудови сучасної системи захисту мовної інформації в умовах зростання технічних можливостей несанкціонованого перехоплення.

1.4. Організаційні та режимні заходи

Технічний захист мовної інформації з обмеженим доступом - це комплекс організаційних і технічних заходів, що здійснюються у приміщеннях, спеціально виділених для роботи з мовною інформацією з обмеженим доступом. Не допускається експлуатація зазначених приміщень без спеціального обстеження їх і встановленого в них обладнання з метою визначення можливості формування технічних каналів витоку інформації з обмеженим доступом [4].

Режимні заходи є невід'ємною складовою конкретної системи захисту мовної інформації і спрямовані на мінімізацію ризику витоку інформації через людський фактор та забезпечення контролю за використанням приміщення. Основу цих заходів складає регламент доступу, який передбачає обмеження кола осіб, що мають право перебувати в контрольованій зоні, а також контроль за переміщенням персоналу всередині приміщення, що дозволяє запобігати несанкціонованому спостереженню або запису мовного сигналу.

Важливим організаційно-технічним елементом захисту інформації є встановлення правил щодо використання мобільних пристроїв та інших електронних засобів у контрольованих приміщеннях, оскільки вони можуть виступати технічними каналами витоку інформації, а також проведення регулярної

перевірки і сертифікації технічного обладнання з метою виявлення несанкціонованих модифікацій або сторонніх пристроїв. [5] Порядок проведення конфіденційних переговорів передбачає чітке планування часу та місця їх проведення, підготовку приміщення до забезпечення оптимальної акустичної ізоляції та використання технічних засобів маскування сигналу, що забезпечує збереження розбірливості мовлення лише для дозволених осіб.

Система організаційних заходів також включає регулярний аудит ефективності застосованих технічних засобів, перевірку стану звукопоглинальних конструкцій, контроль за роботою активних систем маскування та оцінку залишкового ризику витоку мовної інформації. Додатково, режимні заходи передбачають стандарти поведінки персоналу, включаючи заборону на ведення конфіденційних розмов у несанкціонованих зонах, навчання співробітників правилам захисту інформації та підтримку дисципліни щодо дотримання встановлених процедур.

Комплексне застосування організаційних і режимних заходів забезпечує не лише контроль над середовищем і персоналом, а й підвищує ефективність технічних методів захисту, створюючи інтегровану систему, здатну мінімізувати ризики витоку мовної інформації та підтримувати високий рівень конфіденційності в контрольованому приміщенні.

Організаційні та режимні заходи передбачають також розробку чіткої системи процедур і протоколів [6], які регламентують підготовку та проведення конфіденційних заходів у приміщенні, включаючи визначення часу доступу, оптимальних маршрутів пересування персоналу та розташування учасників переговорів для зниження ризику акустичного перехоплення. Важливим аспектом є планування чергувань та зон відповідальності співробітників, що дозволяє мінімізувати несанкціоноване спостереження та забезпечує контроль за дотриманням правил поведінки всередині приміщення. Система організаційних заходів передбачає впровадження регулярних процедур аудиту, включно з перевіркою дотримання внутрішніх регламентів, оцінкою стану обладнання та ефективності заходів безпеки, а також формування звітності для керівництва з

метою оцінки ризиків і вдосконалення процедур.

Особливу увагу приділяють аналітичному підходу до оцінки ефективності заходів, коли на основі збору даних про рівень шуму, поведінку персоналу та роботу технічних систем формуються висновки щодо необхідності додаткових коригувальних дій. Також застосовуються методи моделювання сценаріїв витоку інформації через людський фактор, включно з аналізом дій співробітників у нестандартних ситуаціях, наприклад, під час перевантаження або технічних збоїв. На основі таких досліджень розробляються рекомендації щодо оптимізації процедур доступу, посилення контролю за переміщенням персоналу та уточнення правил використання інформаційних та електронних носіїв.

Організаційні заходи захисту інформації передбачають систематичне навчання персоналу з використанням практичних кейсів і тренінгів, що імітують реальні загрози витоку інформації, а також інтеграцію отриманих знань і навичок у повсякденну діяльність співробітників [7]. Такий підхід дозволяє створити культуру безпеки, де кожен учасник розуміє свою відповідальність та роль у підтриманні конфіденційності. Інтеграція аналітичних процедур, регулярного навчання та контролю за виконанням регламентів забезпечує постійне вдосконалення системи організаційних і режимних заходів, що є критично важливим для підтримки високого рівня безпеки мовної інформації у динамічних умовах експлуатації приміщення.

У перспективі вдосконалення організаційних та режимних заходів велике значення має інтеграція сучасних технологій контролю та моніторингу, які дозволяють підвищити ефективність захисту мовної інформації та мінімізувати людський фактор. До таких технологій належать автоматизовані системи контролю доступу, що фіксують і обмежують вхід до приміщення на основі біометричних даних або електронних пропусків, а також датчики присутності, що дозволяють визначати реальну кількість осіб у контрольованій зоні та відстежувати їхнє переміщення. Системи відеоспостереження з аналітикою поведінки можуть виявляти порушення встановлених правил та попереджати про потенційні ризики витоку інформації, а автоматизовані журнали подій дозволяють проводити

швидкий аналіз дій персоналу у разі інциденту. Використання інтегрованих платформ для моніторингу та аудиту режимів доступу і функціонування технічних засобів захисту забезпечує своєчасне виявлення вразливих місць системи безпеки, дає змогу оцінювати ефективність встановлених процедур та впроваджувати коригувальні заходи без зниження рівня конфіденційності інформації [8]. Розвиток таких технологій відкриває можливості для створення динамічних систем управління безпекою, що автоматично адаптуються до змін умов експлуатації приміщення та забезпечують постійний контроль за дотриманням режимів конфіденційності, підвищуючи надійність захисту мовної інформації в сучасних умовах.

1.5 Комплексний підхід до інтеграції системи

Комплексний підхід до інтеграції системи захисту мовної інформації передбачає об'єднання всіх компонентів безпеки приміщення — геометричних і акустичних характеристик, каналів потенційного витоку, технічних засобів захисту, організаційних та режимних заходів — у єдину скоординовану систему, яка забезпечує максимальний рівень конфіденційності та мінімізацію ризиків перехоплення інформації. Інтеграція починається з аналізу фізичних параметрів приміщення та виявлення всіх можливих шляхів витоку мовного сигналу, після чого здійснюється комплексне планування розміщення звукопоглинальних конструкцій, меблів та перегородок у поєднанні з технічними засобами активного маскування, що забезпечує контрольований розподіл акустичної енергії. Одночасно впроваджуються організаційні та режимні заходи, які регламентують доступ до приміщення, порядок проведення конфіденційних переговорів, поведінку персоналу та використання електронних пристроїв, що створює контрольовану соціально-технічну середу.

Координація всіх компонентів системи досягається шляхом розробки інтегрованих протоколів, де дії пасивних і активних засобів захисту поєднуються з режимними процедурами, автоматизованим контролем доступу та моніторингом стану приміщення. Використання сучасних технологій дозволяє проводити

динамічний аналіз ефективності заходів у реальному часі, виявляти слабкі місця та оперативно коригувати систему безпеки без зниження рівня захисту. Особливо важливо враховувати взаємодію фізичних бар'єрів, акустичних панелей та систем маскування зі схемами організаційного контролю та поведінки персоналу, оскільки саме комбінація технічних і соціальних заходів забезпечує комплексну протидію витоку мовної інформації через різні канали.

Додатковим елементом інтеграції є застосування аналітичних методів оцінки ризиків, включаючи моделювання сценаріїв потенційного витоку та симуляційних перевірок ефективності технічних і організаційних заходів, що дозволяє формувати науково обґрунтовані рекомендації щодо удосконалення системи. Такий комплексний підхід дозволяє не лише мінімізувати ймовірність перехоплення інформації, а й забезпечує адаптивність системи до змін у конфігурації приміщення, змін умов експлуатації та появи нових загроз, створюючи вискоелективну та надійну систему захисту мовної інформації в контрольованому приміщенні.

1.6 Висновки

Підсумовуючи результати дослідження акустичних властивостей приміщення, можна стверджувати, що саме характеристики простору та матеріалів визначають базовий рівень ризику витоку мовної інформації, а тому їхнє вивчення є фундаментальним етапом побудови системи захисту. Основні канали витоку мовної інформації узагальнено в таблиці 1.

Таблиця 1 Основні канали витоку мовної інформації

Акустичний	Передача звуку повітрям
Віброакустичний	Передача коливань конструкціями
Електроакустичний	Перетворення звуку в сигнал
Оптичний	Візуальне спостереження
Організаційний	Людський фактор

Встановлено, що геометрія приміщення, наявність кутів, ніш і великих площин істотно впливають на рівень реверберації та напрямки поширення звукових хвиль, формуючи зони підвищеної акустичної активності, які можуть стати джерелом витоку. Виявлено, що матеріали стін, стелі, підлоги та міжповерхових перекриттів мають різний коефіцієнт звукопоглинання, який визначає здатність конструкцій пропускати або утримувати мовний сигнал, що дозволяє оцінити їхню стійкість до неконтрольованої передачі звуку. Крім того, проведений аналіз підтвердив, що вентиляційні канали, технічні порожнини, щілини та місця проходження комунікацій здатні значно посилювати акустичну проникність будівлі, створюючи небажані шляхи поширення звукової інформації за межі контрольованої зони. Важливим результатом дослідження стало встановлення залежності між характеристиками відбиття та поглинання звуку і ефективністю подальших технічних засобів захисту, оскільки саме точні акустичні параметри визначають доцільність використання певних матеріалів, пристроїв активного шумового маскування та способів оптимізації внутрішнього простору. Таким чином, аналіз акустичних властивостей формує науково обґрунтовану основу для проектування комплексної системи захисту мовної інформації, дозволяючи визначити критичні ділянки, оцінити масштаб ризиків і забезпечити вибір адекватних заходів безпеки.

Підсумовуючи результати визначення каналів витоку мовної інформації, можна зазначити, що детальна ідентифікація всіх можливих шляхів поширення мовного сигналу є критично важливою для формування ефективної системи безпеки, оскільки саме від правильності цього етапу залежить здатність приміщення протистояти як пасивному, так і активному перехопленню. Дослідження показало, що найбільш небезпечними каналами витоку є конструктивні елементи будівлі, до яких належать вентиляційні шахти, технологічні отвори, міжкімнатні шви, розетки та місця проходження комунікацій, адже вони здатні передавати як повітряні, так і структурні акустичні коливання на значні відстані. Було встановлено, що дверні та віконні блоки, нещільні прилягання рам і слабо ізольовані стики можуть створювати додаткові повітряні канали

витоку, тим самим дозволяючи мовному сигналу потрапляти у суміжні приміщення або на зовнішні ділянки будівлі. Окрему групу загроз становлять інженерні мережі та конструктивні елементи, які мають властивість передавати віброакустичні коливання, через що навіть наявність масивних стін не гарантує абсолютної ізоляції. Додатковим фактором ризику є можливість використання спеціальних технічних засобів прослуховування, здатних знімати інформацію через вібрації поверхонь або електромагнітні перешкоди. Комплексне дослідження цих каналів дозволило сформулювати об'єктивне уявлення про найбільш вразливі точки приміщення та визначити першочергові напрямки для впровадження технічних, конструктивних і режимних засобів захисту, що створює підґрунтя для подальшого проектування інтегрованої системи безпеки.

Ефективна система технічного захисту в контрольованому приміщенні базується на комплексному поєднанні різних технологічних рішень, спрямованих на мінімізацію можливості перехоплення акустичних сигналів як усередині приміщення, так і за його межами. У межах розділу підкреслено, що ключову роль відіграють електроакустичні генератори шуму, здатні створювати фон, який унеможливорює виділення корисної мовної інформації на тлі перешкод. Додатково значущими є системи вібродемпфування, які знижують рівень структурних коливань і зменшують ризик передачі звуку через будівельні конструкції. Важливим елементом комплексного захисту виступають спеціалізовані шумоізоляційні матеріали, які формують фізичний бар'єр для поширення звуку. Окремо відзначено роль технічних засобів моніторингу, що дозволяють контролювати акустичний фон, виявляти потенційні закладки або аномальні джерела витоку, а також забезпечувати постійну діагностику ефективності встановлених систем. У сукупності всі ці засоби створюють багаторівневий технічний контур захисту, який значно ускладнює можливість несанкціонованого зняття інформації та забезпечує стабільний рівень безпеки мовних комунікацій.

Належно вибудована система управління, контролю та регламентації визначає реальну дієвість захисту мовної інформації, виступаючи ключовою опорою для всіх технічних та акустичних рішень. У підсумку можна зазначити, що

цей розділ висвітлює необхідність формування чіткої структури доступу до контрольованого приміщення, включно з визначенням категорій осіб, які мають право перебувати в ньому, порядку їх реєстрації, перевірки та контролю часу перебування. Важливим аспектом є створення режиму роботи приміщення, що передбачає регулярні огляди, інспекцію обладнання, перевірку на наявність підозрілих пристроїв, а також документування всіх дій, пов'язаних із функціонуванням системи захисту. Розділ також підкреслює значення людського фактора, адже непроінформований або неуважний співробітник може створити критичну вразливість, яку не компенсують навіть найсучасніші технічні засоби. Тому важливими складовими режиму стають навчання персоналу, формування культури інформаційної безпеки, проведення інструктажів і моделювання сценаріїв потенційних загроз. Класифікацію основних методів захисту мовної інформації наведено в таблиці 2.

Таблиця 2 Основні канали витоку мовної інформації

Пасивні	Обмеження поширення звуку
Активні	Маскування сигналу
Технічні	Апаратні засоби
Організаційні	Регламентация доступу
Комплексні	Поєднання методів

Зрозуміло, що організаційні та режимні заходи не лише забезпечують контрольований доступ і дисципліну, але й створюють передумови для оперативного виявлення інцидентів, швидкого реагування на ризики та постійного підтримання системи захисту в актуальному стані. У результаті саме цей комплекс процедур і правил дозволяє гарантувати, що всі технічні, акустичні та структурні методи захисту працюють узгоджено, а приміщення залишається стійким до зовнішніх і внутрішніх загроз перехоплення мовної інформації.

Самі по собі окремі технічні засоби, акустичні рішення або організаційні

заходи не здатні забезпечити достатній рівень безпеки, якщо вони впроваджуються розрізнено, без взаємної адаптації та контролю сумісності. Комплексний підхід передбачає поєднання аналізу акустичних характеристик приміщення, оцінки потенційних каналів витоку, вибору оптимальних технічних засобів і встановлення режимних вимог у цілісну модель, що функціонує за єдиними правилами та алгоритмами. Під час узагальнення цього розділу особлива увага приділяється тому, що інтеграція має не просто враховувати окремі особливості приміщення, а й бути динамічною — тобто такою, що дозволяє адаптувати систему до змін у технологіях, нових загрозах, модернізації обладнання або зміні умов експлуатації. Також підкреслюється необхідність координації між технічними фахівцями, адміністративним персоналом і відповідальними за безпеку особами, адже ефективність комплексного підходу визначається не лише апаратними чи програмними рішеннями, а саме узгодженістю та безперервністю взаємодії між усіма учасниками процесу. Таким чином, розділ демонструє, що інтегрована система захисту — це не статичний набір компонентів, а гнучкий, багаторівневий механізм, який забезпечує максимальну стійкість приміщення до витоку мовної інформації завдяки поєднанню технічних, акустичних, організаційних і процедурних заходів у єдину безперервну структуру.

Розділ 2

АНАЛІЗ АКУСТИЧНИХ ВЛАСТИВОСТЕЙ КОНТРОЛЬОВАНОГО ПРИМІЩЕННЯ ТА ЗАГРОЗ ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ

2.1. Фізичні основи поширення звуку у приміщеннях

Поширення звуку в замкненому просторі є складним акустичним процесом, який визначає рівень небезпеки витоку мовної інформації. В замкнених просторах поширення звуку підпорядковується законам хвильової фізики, при цьому істотний вплив мають геометрія приміщення та властивості огорожувальних конструкцій [9]. У контрольованому приміщенні, що спеціально призначене для ведення конфіденційних переговорів або оброблення чутливих даних, навіть незначні акустичні особливості здатні впливати на якість захищеності. Звук, як механічне коливання частинок повітря, підпорядковується законам хвильової фізики, тому його поведінка в обмеженому просторі відрізняється від поведінки у відкритому середовищі. Кожен елемент конструкції, кожна поверхня і навіть розташування меблів формують унікальну акустичну картину, яка може або підсилювати конфіденційність, або, навпаки, сприяти поширенню небажаного сигналу за межі приміщення.

Важливою особливістю звуку є його здатність змінювати характеристики залежно від частоти. Високочастотні компоненти сигналу швидко втрачають енергію та сильніше поглинаються повітрям. Низькочастотні акустичні хвилі мають значну довжину хвилі, що дозволяє їм огинати перешкоди та проникати крізь конструктивні елементи будівель [10]. У мовному діапазоні низькі та середні частоти несуть основну енергетичну складову, тому є найбільшим джерелом потенційного витоку. Високі частоти, хоч і слабші за енергією, забезпечують чіткість та розбірливість мовлення; саме вони дозволяють підслуховуючим пристроям відтворювати зміст фраз навіть на значних відстанях.

Поведінка звуку значною мірою залежить від акустичної взаємодії хвиль із поверхнями. У приміщеннях постійно відбувається відбиття звукових хвиль від

стін, підлоги та стелі. Ці відбиття можуть накладатися одне на одне, утворюючи складні інтерференційні картини. В окремих точках приміщення можуть виникати вузли та пучності стоячих хвиль, де рівень звуку суттєво змінюється. Зони підсилення сигналу є особливо небезпечними, оскільки вони можуть створювати ділянки з підвищеним рівнем звукового тиску в точках, які межують зі щілинами, вентиляційними каналами або тонкими ділянками стін. У таких місцях імовірність витоку інформації значно зростає.

Відбиття звуку також визначають час реверберації приміщення — проміжок, за який рівень звукової енергії зменшується на 60 дБ після припинення джерела. Якщо час реверберації є надто великим, виникає ефект «луни», що підвищує загальний рівень звуку всередині приміщення та полегшує перехоплення мовного сигналу технічними засобами. З іншого боку, надмірне поглинання також небажане, оскільки призводить до різкої зміни спектру мови та може ускладнити оцінку реальних акустичних властивостей приміщення. Тому оптимальний рівень звукопоглинання має враховувати баланс між розбірливістю мовлення, комфортом та захищеністю.

Проникнення звуку через будівельні конструкції залежить не лише від їхньої маси, а й від механічних властивостей матеріалу. Будь-яка стіна або перегородка може поводитися як мембрана, що передає частину акустичної енергії у вигляді вібрацій. Навіть якщо звуковий тиск у приміщенні порівняно невеликий, у певних частотних діапазонах конструкції можуть входити в резонанс, що істотно послаблює їхній захист. Особливо вразливими є легкі перегородки з гіпсокартону або скла, які мають низький опір до деяких мовних частот. Також важливим є той факт, що будь-який отвір у конструкції — розетка, слаботочний канал, технологічна щілина, навіть незначний за розмірами, — може стати «акустичним провідником», через який звук передаватиметься значно ефективніше, ніж через саму площину стіни.

Віброакустичне поширення звуку є додатковим джерелом загрози. Будівельні конструкції здатні передавати механічні коливання на значні відстані. Частина мовного сигналу перетворюється на вібрації, які рухаються по стінах,

перекриттях та інших жорстких елементах. У суміжних приміщеннях ці коливання можуть бути легко перетворені назад на звук за допомогою контактних або лазерних мікрофонів. Особливо небезпечними є вентиляційні та водопровідні труби, які виконують роль своєрідних хвилеводів. Вони здатні передавати низькочастотні компоненти мовлення майже без спотворень, створюючи приховані канали витоку інформації.

Значну роль у формуванні загального акустичного середовища відіграє і наповнення приміщення предметами інтер'єру. Меблі, техніка, декоративні елементи, навіть розташування людей можуть змінювати розподіл хвиль, поглинати або відбивати акустичну енергію. Наявність великої кількості твердих предметів з рівними поверхнями сприяє багаторазовим відбиттям та зростанню реверберації. М'які меблі, тканинні елементи чи килими навпаки зменшують рівень хвильової активності. У контексті технічного захисту інформації це означає, що будь-які зміни в інтер'єрі можуть вплинути на рівень реальної захищеності приміщення і мають враховуватись при проведенні акустичного обстеження.

Таким чином, поширення звуку в приміщенні є комплексним процесом, у якому одночасно діють повітряні та віброакустичні хвилі, інтерференція, реверберація, резонансні явища та властивості будівельних матеріалів. Врахування всіх цих факторів є необхідною умовою для подальшого формування ефективної системи захисту мовної інформації. Досконале розуміння механізмів передачі звуку дозволяє прогнозувати канали витоку, визначати слабкі місця огорожувальних конструкцій та обирати адекватні технічні та організаційні засоби захисту.

Додатковим аспектом, який суттєво впливає на поширення звуку та ризики його витоку, є температура та вологість повітря в приміщенні. Фізичні властивості повітря змінюють швидкість звуку, щільність середовища та ступінь поглинання високочастотних компонентів. За підвищеної температури повітря звук поширюється швидше, а втрати енергії зменшуються, що може збільшувати потенційну дальність поширення мовного сигналу за межі приміщення. Вологе повітря поглинає менше високочастотних коливань, зберігаючи розбірливість мови

на більшій відстані. У реальних умовах ці фактори можуть змінюватися протягом дня, особливо у приміщеннях з кондиціонуванням або природною вентиляцією. Внаслідок цього рівень захищеності приміщення не є статичним і потребує періодичного контролю, особливо у критичних зонах, де технічні засоби перехоплення можуть бути розміщені найбільш імовірно.

Важливим явищем, яке необхідно враховувати під час аналізу поширення звуку, є дифракція — здатність хвиль огинати перешкоди та проникати у зони, що не мають прямої видимості. Саме завдяки дифракції звук може потрапляти у коридори, технічні шахти, вентиляційні канали або під стелі, навіть якщо ці елементи розташовані під значним кутом до джерела звуку. У контрольованих приміщеннях це створює загрозу появи «неочевидних» каналів витоку, які можуть залишатися непомітними при поверхневому обстеженні. Більш того, дифраговані хвилі можуть втрачати напрямленість, але зберігати достатню амплітуду для перехоплення спеціальними мікрофонами, що працюють у широкому частотному діапазоні.

У контексті захисту мовної інформації особливої уваги заслуговує таке явище як механічний зв'язок між конструкціями будівлі. Сучасні будівельні конструкції часто мають складну структуру: суміщені каркаси, подвійні перегородки, натяжні стелі, підлогові системи із різними шарами матеріалів. Акустичні коливання можуть збуджувати структурні вібрації будівельних елементів, які стають вторинними джерелами випромінювання звуку [11]. Навіть за наявності якісної звукоізоляції між приміщеннями можливе виникнення жорстких акустичних «містків» — вузьких зон, через які звукові вібрації передаються значно ефективніше, ніж через основну площину стіни. Такими містками можуть бути металеві профілі, елементи каркаса, кріплення дверних коробок, стики плит перекриттів або навіть системи кондиціонування. Якщо під час проектування або ремонту приміщення не було враховано віброакустичні властивості таких елементів, вони створюють суттєвий ризик витоку мовної інформації.

Окремо слід зазначити вплив ефекту резонансу у порожнинах та каналах, які

часто залишаються в конструкціях будівель. Порожнини в стінах, фальшпідлогах або підвісних стелях можуть працювати як резонатори, підсилюючи певні частоти мовного сигналу. Наприклад, ефект резонансу Гельмгольца дозволяє невеликій порожнині з вузьким отвором значно посилювати звукові коливання, які потрапляють у резонансний діапазон. У практиці технічного захисту траплялися випадки, коли непомітні конструктивні об'єми, залишені будівельниками, ставали підсилювачами небезпечного акустичного каналу. Тому детальне обстеження порожнин, стиків і незаповнених технічних ніш є обов'язковою частиною аналізу приміщення.

З погляду безпеки значною загрозою є також переважання відбитих хвиль над прямим звуком. Якщо у приміщенні багато твердих поверхонь, а час реверберації довгий, у деяких зонах може виникати акустичне підсилення, яке неочевидне для особи, що перебуває у приміщенні. Людина може відчувати комфортне акустичне середовище, але відбитий звук потенційно посилюється і передається через слабкі ділянки конструкцій. Підслуховуючі пристрої в таких зонах фіксують сигнал значно якісніше, ніж безпосередньо біля джерела звуку.

Сучасні засоби технічної розвідки здатні використовувати навіть незначні акустичні коливання для відновлення мовної інформації. Лазерні мікрофони зчитують вібрації від поверхонь, спрямовані мікрофони аналізують відбиті хвилі, а алгоритми цифрової обробки сигналів здатні відтворювати фрази навіть із суттєво зашумлених сигналів. Тому фізичні властивості поширення звуку в приміщеннях потрібно розглядати у контексті сучасних загроз, які використовують не лише пряме прослуховування, а й відновлення сигналу з мінімальних фрагментів.

Нарешті, важливо враховувати, що реальне акустичне середовище приміщення формується не лише фізичними процесами поширення хвиль, а й динамічними умовами: переміщенням людей, відкриванням дверей, роботою техніки, вентиляції, ліфтів або зовнішнім шумовим середовищем. Ці фактори можуть створювати як додаткову маскувальну дію, так і виникнення імпульсів, які тимчасово відчиняють канали передачі звуку. Для прикладу, звук від відкриття дверей створює короткочасний низькочастотний імпульс, який може підсилити

вібрації стін у резонансному діапазоні, роблячи можливим витік інформації саме в цей момент. Аналогічно, запуск системи вентиляції може змінювати параметри акустичного хвилеводу і тимчасово збільшувати його пропускну здатність для окремих частот мовного сигналу.

Таким чином, поширення звуку в контрольованому приміщенні є великою сукупністю взаємопов'язаних процесів, які охоплюють фізику хвиль, властивості будівельних матеріалів, резонансні та віброакустичні явища, а також поведінку середовища у реальних експлуатаційних умовах. Основні фактори, що впливають на поширення мовної інформації в приміщенні, наведено в таблиці 3. Глибоке розуміння цих процесів є фундаментом для подальшого аналізу каналів витоку мовної інформації та розроблення ефективних методів її захисту.

Таблиця 3 Основні фактори, що впливають на поширення мовної інформації в приміщенні

Об'єм приміщення	Розміри, висота
Матеріали стін	Бетон, гіпсокартон
Отвори	Двері, вентиляція
Меблі	Поглинання звуку
Рівень шуму	Фоновий шум

2.2 Акустичні параметри контрольованого приміщення

Акустичні параметри контрольованого приміщення є визначальними для формування рівня захищеності мовної інформації, оскільки саме вони визначають умови поширення, відбиття, поглинання та проникнення звукових хвиль. На відміну від загальних фізичних закономірностей поширення звуку, які мають універсальний характер, акустичні параметри конкретного приміщення

формуються його геометрією, будівельними матеріалами, конструктивними особливостями та умовами експлуатації. Їх аналіз дозволяє не лише оцінити потенційні канали витоку інформації, а й обґрунтувати технічні рішення щодо створення ефективної системи захисту.

Першочерговим параметром контрольованого приміщення є його геометричні характеристики. Площа, об'єм, співвідношення довжини, ширини та висоти безпосередньо впливають на формування акустичного поля. У прямокутних приміщеннях часто виникає регулярна система стоячих хвиль, обумовлена кратністю розмірів, тоді як у приміщеннях складної форми спостерігається хаотичний розподіл звукового тиску. Наявність колон, ніш, перегородок і декоративних конструкцій викликає локальні акустичні ефекти, що можуть як зменшувати, так і збільшувати ймовірність утворення небезпечних зон. Особливо важливими є відстані між протилежними поверхнями, оскільки саме вони визначають основні модальні частоти приміщення.

Суттєвий вплив на акустичні властивості мають матеріали, з яких виконані огорожувальні конструкції. Кожен матеріал характеризується коефіцієнтом звукопоглинання, що залежить від частоти. Бетонні та цегляні стіни володіють високим коефіцієнтом відбиття, тому сприяють збереженню звукової енергії всередині приміщення. Навпаки, пористі матеріали, такі як мінеральна вата, пробка, текстильні панелі або спеціалізовані акустичні плити, значно зменшують рівень відбитого сигналу. Тип підлогового покриття також має помітний вплив: килимові покриття сприяють додатковому поглинанню, тоді як тверді поверхні, зокрема ламінат або керамічна плитка, формують інтенсивні відбиття. Сукупність цих параметрів формує загальний акустичний «портрет» приміщення.

Одним з ключових інтегральних параметрів є час реверберації, який визначається як час зменшення рівня звукового тиску на 60 дБ після припинення роботи джерела звуку. Цей параметр безпосередньо пов'язаний із розбірливістю мовлення та рівнем акустичного комфорту. У контрольованих приміщеннях надмірно великий час реверберації призводить до накопичення відбитих хвиль, що збільшує загальний рівень звукового фону та потенційну дальність поширення

мовної інформації. Надто малий час реверберації, у свою чергу, може вказувати на надмірне акустичне «заглушення», що хоча й знижує витік інформації, проте може викривляти спектр мовлення і ускладнювати коректну оцінку акустичних характеристик приміщення при проведенні вимірювань.

Важливим параметром також є рівень фонових шумів у приміщенні. Він формується як внутрішніми джерелами, такими як вентиляційні установки, комп'ютерна техніка, освітлювальні системи, так і зовнішніми факторами: транспортним шумом, роботою сусідніх приміщень, інженерних систем будівлі. З одного боку, наявність фонового шуму може виконувати захисну функцію, маскуючи мовний сигнал і ускладнюючи його перехоплення. З іншого боку, нестабільний або імпульсний шум здатний створювати умови, за яких сучасні цифрові системи обробки сигналу можуть ефективно відновлювати мову методом спектрального аналізу та фільтрації.

Окрему увагу необхідно приділити просторовому розподілу звукового тиску. У реальних умовах рівень звуку не є однорідним у всьому об'ємі приміщення. У різних зонах можуть формуватися області акустичного підсилення та ослаблення, що обумовлено інтерференційними процесами. Такі ділянки мають різний рівень інформативності мовного сигналу, тому деякі частини приміщення є більш уразливими з точки зору витоку. Саме в цих «критичних точках» найдоцільніше розміщувати засоби моніторингу або, навпаки, посилювати захисні конструкції.

Ще одним важливим параметром є коефіцієнт звукоізоляції огорожувальних конструкцій, який кількісно описує здатність стін, перекриттів і перегородок зменшувати рівень звукового тиску при передачі сигналу в суміжні приміщення. Він залежить від товщини, щільності матеріалу, наявності повітряних проміжків, а також якості монтажу. Навіть матеріали з високими паспортними характеристиками можуть втрачати ефективність на практиці через дефекти монтажу, перекося, тріщини, неущільнені стики або технологічні отвори. Тому реальні акустичні параметри контрольованого приміщення часто відрізняються від розрахункових і потребують експериментального підтвердження.

Суттєвим фактором є також наявність та характеристики інженерних

комунікацій, які можуть виступати в ролі акустичних хвилеводів. Вентиляційні канали, системи кондиціювання, водопровідні та опалювальні труби мають властивість передавати як повітряні, так і віброакустичні коливання. Їхні діаметр, довжина, матеріал та спосіб кріплення безпосередньо впливають на рівень ослаблення сигналу. У багатьох випадках саме інженерні системи є найбільш вразливими елементами конструкції з точки зору витоку мовної інформації.

Акустичні параметри приміщення не є постійними у часі. Вони змінюються залежно від заповненості приміщення людьми, розташування меблів, режиму роботи технічних систем та навіть погодних умов. Зміна кількості людей у приміщенні змінює коефіцієнти поглинання, оскільки людське тіло і одяг діють як додаткові поглиначі звуку. Відкриття або закриття дверей, зміна режиму вентиляції або переміщення мобільних перегородок також впливають на реальні умови поширення звукових хвиль. Це означає, що оцінка акустичних параметрів контрольованого приміщення повинна здійснюватися з урахуванням різних сценаріїв його експлуатації.

Таким чином, акустичні параметри контрольованого приміщення являють собою багатофакторну систему взаємопов'язаних характеристик, які формують реальні умови поширення мовлення та визначають рівень захищеності інформації. Їх детальний аналіз є необхідним етапом перед розробленням та впровадженням технічних і організаційних заходів захисту мовної інформації, що будуть розглянуті у наступних підрозділах роботи.

Додатково до вже наведених характеристик, важливим акустичним параметром контрольованого приміщення є частотна характеристика середовища, яка описує вибіркове послаблення або підсилення окремих діапазонів частот. У реальних умовах приміщення не є акустично нейтральним: воно виступає як своєрідний фільтр, що нерівномірно впливає на спектр мовного сигналу. Деякі частоти можуть пригнічуватися за рахунок поглинання матеріалами, інші — підсилюватися завдяки резонансним явищам. Така вибіркковість створює спотворення сигналу, які, з одного боку, можуть ускладнювати його пряме сприйняття, а з іншого — можуть бути компенсовані сучасними алгоритмами

цифрової обробки сигналів, що підвищує актуальність поглибленого частотного аналізу акустичних умов.

Параметри дифузності звукового поля також суттєво впливають на рівень захищеності приміщення. Дифузним звуковим полем називають таке звукове поле в замкненому приміщенні, в якому звукова енергія рівномірно розподілена в усіх напрямках, а ймовірність поширення звукових хвиль є однаковою незалежно від напрямку їх розповсюдження [12]. Дифузне звукове поле характеризується рівномірним розподілом енергії по всьому об'єму, що знижує ймовірність виникнення локальних зон високого акустичного тиску. Водночас у приміщеннях з низьким рівнем дифузності формуються напрямлені акустичні потоки, які можуть «спрямовувати» енергію звуку до слабких ділянок огорожувальних конструкцій або до інженерних отворів. У контексті захисту мовної інформації це означає, що недостатня дифузність поля підвищує ризик спрямованого витоку сигналу.

Окрему увагу необхідно приділити такому параметру, як коефіцієнт передачі структурного шуму. Він характеризує здатність коливань передаватися через тверді елементи конструкцій — балки, перекриття, металеві каркаси, кріпильні елементи. На практиці структурний шум часто поширюється значно ефективніше за повітряний, особливо в низькочастотному діапазоні. Контроль цього параметра дозволяє оцінити небезпеку витоку через віброакустичні канали та виявити так звані «акустичні мости» між приміщеннями.

Також значення має характеристика добротності акустичних резонансів. Чим вища добротність резонансної системи, тим вузькіший частотний діапазон підсилення, але тим більша амплітуда коливань у резонансній області. У контексті захисту мовної інформації це означає, що навіть незначні гармоніки мовлення можуть суттєво підсилюватися в окремих ділянках приміщення або в конструктивних елементах, що створює потенційні умови для перехоплення сигналу за межами контрольованої зони.

Істотний вплив на акустичні параметри має стан будівельних конструкцій. Тріщини, мікрощілини, ослаблені кріплення, зношені ущільнювачі дверей і

віконних блоків суттєво знижують фактичний рівень звукоізоляції. З часом ці дефекти накопичуються, що призводить до деградації захисних властивостей навіть у приміщеннях, які спочатку проектувалися як спеціалізовані. Тому оцінка акустичних параметрів повинна розглядатися як безперервний процес, що включає періодичні перевірки та коригування.

Слід також відзначити роль електромеханічних пристроїв, розташованих у приміщенні, у формуванні акустичних властивостей. Динаміки, мікрофони, системи гучномовного зв'язку, навіть вимкнені аудіопристрої можуть виступати в ролі пасивних резонаторів, що взаємодіють із звуковим полем. Деякі електронні компоненти здатні ненавмисно перетворювати акустичні коливання на електричні сигнали, що створює додаткові ризики витоку через побічні канали.

Важливим параметром є також стабільність акустичних характеристик у часі. Для контрольованих приміщень критичним є не лише середній рівень звукоізоляції, а й відсутність раптових змін у характеристиках середовища. Наприклад, коливання температури можуть призводити до деформацій матеріалів, а зміни вологості — до зміни коефіцієнтів поглинання. Це може викликати непередбачувані зміни в поведінці звукових хвиль і тимчасове зниження рівня захищеності.

Таким чином, акустичні параметри контрольованого приміщення являють собою складну, багатовимірну систему характеристик, яка охоплює геометричні, матеріальні, частотні, структурні та експлуатаційні аспекти. Їх комплексний аналіз дозволяє не лише оцінити фактичний рівень захищеності мовної інформації, а й створити науково обґрунтовану базу для розроблення практичних заходів з підвищення ефективності системи захисту.

2.3 Оцінка рівня загроз для конкретного приміщення

Оцінка рівня загроз базується на співвідношенні можливостей потенційного порушника та властивостей середовища [13]. Відповідно, оцінка рівня загроз витоку мовної інформації в контрольованому приміщенні є ключовим етапом

формування ефективної системи захисту, оскільки саме на цьому етапі визначається ймовірність реалізації потенційних каналів витоку та ступінь небезпеки втрати конфіденційності. Комплексна оцінка загроз базується на аналізі фізичних характеристик приміщення, особливостях поширення акустичних коливань, а також можливостях сучасних технічних засобів перехоплення інформації. Основним завданням даного етапу є встановлення гранично допустимих рівнів акустичного сигналу за межами контрольованої зони та визначення умов, за яких мовна інформація стає доступною для несанкціонованого сприймання.

Процес оцінки загроз передбачає формування акустичної моделі приміщення, яка враховує його геометричні параметри, об'єм, площу огорожувальних конструкцій, типи та акустичні характеристики матеріалів. На основі цих даних визначаються коефіцієнти ослаблення звуку при проходженні через стіни, перекриття, двері та інші елементи конструкції. Особлива увага приділяється частотному діапазону мовного сигналу, оскільки низькочастотні компоненти мови характеризуються вищою проникною здатністю та меншою залежністю від поверхневих властивостей матеріалів. Розрахункові моделі дозволяють прогнозувати рівень звукового тиску в суміжних приміщеннях та за межами будівлі, що є основою для подальшої класифікації рівня загрози.

Важливим елементом оцінювання є визначення співвідношення сигнал/шум у потенційних точках перехоплення. Для цього враховується як рівень корисного мовного сигналу, так і фоновий акустичний шум, який формується зовнішніми джерелами, такими як транспортні потоки, робота вентиляційних систем, електротехнічне обладнання та інші фактори. Якщо відношення рівня мовного сигналу до фонових шумів перевищує критичні значення, мовна інформація може бути частково або повністю розбірливою. Саме тому оцінка загроз не обмежується лише вимірюванням абсолютних рівнів звукового тиску, а обов'язково включає аналіз спектрального складу шуму та його маскуючих властивостей.

Віброакустичні впливи на конструктивні елементи будівель створюють умови для поширення мовної інформації через тверді тіла, що робить необхідним

аналіз коливальних процесів у стінах, перекриттях та інженерних конструкціях при оцінюванні загроз витоку інформації [14]. Для цього досліджуються рівні механічних коливань на поверхнях стін, трубопроводів, вентиляційних каналів та інших елементів, здатних передавати структурні вібрації. Визначаються коефіцієнти передачі коливань у твердих середовищах та можливість їх перетворення назад у акустичний сигнал за межами контрольованого приміщення. При цьому враховується сталий та імпульсний характер коливань, а також резонансні явища, які можуть значно підсилювати певні частотні компоненти мовного сигналу.

Сучасний підхід до оцінки загроз також передбачає аналіз технічних можливостей потенційного порушника. Розглядаються сценарії використання спрямованих мікрофонів, лазерних віброметрів, контактних датчиків і радіотехнічних засобів знімання побічних випромінювань. При цьому враховується дальність дії таких пристроїв, їх чутливість, смуга пропускання та здатність до цифрової обробки сигналів, що дозволяє відновлювати мовну інформацію навіть при низькому первинному рівні сигналу. Таким чином, рівень загрози визначається не лише фізичними параметрами середовища, а й технічним оснащенням потенційного порушника.

Для формалізації результатів оцінювання застосовується система критеріїв і показників, які дозволяють класифікувати ступінь небезпеки витоку мовної інформації. Зазвичай використовуються категорії низького, середнього та високого рівнів загрози, які визначаються на основі значень ослаблення сигналу, співвідношення сигнал/шум та ймовірності успішного перехоплення. На основі цих критеріїв формується загальна карта ризиків для конкретного приміщення, яка відображає найбільш уразливі зони та конструктивні елементи.

Класифікація рівнів загроз дозволяє формалізувати результати аналізу захищеності [15]. Завершальним етапом оцінки рівня загроз є інтегральна оцінка захищеності приміщення, яка базується на поєднанні розрахункових та експериментальних даних. Проводяться контрольні вимірювання рівнів звукового тиску та вібрацій у характерних точках, результати яких зіставляються з

теоретичними моделями. У разі виявлення перевищення безпечних рівнів формуються рекомендації щодо підвищення захищеності. Таким чином, оцінка рівня загроз є не лише аналітичним, а й практично орієнтованим процесом, який забезпечує науково обґрунтовану основу для вибору та оптимізації заходів захисту мовної інформації в контрольованому приміщенні.

Додатково до фізичних характеристик середовища та технічних можливостей потенційного порушника, під час оцінки рівня загроз істотну роль відіграють організаційні та експлуатаційні фактори. Регулярність проведення конфіденційних переговорів, кількість учасників, характер мовного навантаження та тривалість сеансів мовної комунікації впливають на загальний рівень акустичного випромінювання та стабільність формування небезпечних сигналів. Приміщення, у яких систематично проводяться наради з високим рівнем голосового навантаження, мають істотно вищий рівень ризику, ніж приміщення епізодичного використання. Оцінка режиму експлуатації дозволяє більш точно визначити часові інтервали підвищеної вразливості та сформувати профіль загроз у часовому вимірі.

Експериментальні вимірювання є необхідним етапом перевірки адекватності теоретичних моделей [16]. Значна увага у процесі оцінювання приділяється аналізу акустичної стійкості приміщення до навмисних впливів. Розглядаються сценарії, за яких порушник використовує активні методи впливу на середовище, зокрема створення контрольованих акустичних збуджень або використання спеціальних резонансних частот для підсилення передачі мовного сигналу через конструкції. У таких випадках приватний мовний сигнал накладається на штучно сформовані коливання, що може призводити до ефектів модуляції та значного підвищення його доступності на стороні прийому. У межах оцінки загроз аналізується ймовірність реалізації таких сценаріїв та їхня ефективність з урахуванням реальних фізичних обмежень.

Ще одним важливим аспектом є аналіз просторового розташування контрольованого приміщення у будівлі. Приміщення, які межують із вулицею, технічними поверхами, підвалами або суміжними приміщеннями загального користування, як правило, характеризуються підвищеним рівнем ризику. У межах

оцінювання визначаються можливі пункти розміщення технічних засобів перехоплення, враховується доступність цих зон та можливість їх маскування. Просторовий аналіз дозволяє встановити так звані «небезпечні напрямки», з яких найбільш імовірним є перехоплення мовної інформації.

Важливою складовою оцінки є врахування деградації захисних властивостей приміщення з часом. Будівельні матеріали в процесі експлуатації зазнають старіння, утворюються мікротріщини, порушуються герметичні з'єднання, зменшуються показники еластичності ущільнювачів у дверях та вікнах. Усе це призводить до поступового зниження ефективності звукопоглинання та звукоізоляції без проведення будь-яких конструктивних змін. Тому при оцінці рівня загроз вводяться поправочні коефіцієнти, які враховують реальний технічний стан приміщення, а не лише його проєктні характеристики.

Окремого розгляду потребує психологічний фактор, який опосередковано впливає на рівень загроз витоку мовної інформації. Підвищений рівень емоційного напруження учасників переговорів, підвищена гучність мовлення, наявність конфліктних ситуацій або екстрених обговорень можуть істотно збільшувати амплітуду мовного сигналу та кількість інформаційно насичених фрагментів. У процесі оцінки загроз такі фактори також враховуються як змінні, що підвищують імовірність часткового або повного розкриття змісту мовної інформації.

Таким чином, оцінка рівня загроз витоку мовної інформації має багатовимірний характер та поєднує в собі фізико-акустичні, технічні, просторові та людські чинники. Комплексний підхід до оцінювання дозволяє не лише встановити поточний рівень захищеності приміщення, а й спрогнозувати потенційні зміни ризику в разі змін умов експлуатації або появи нових технічних засобів перехоплення. Отримані відповіді формують науково обґрунтовану базу для подальшого проєктування систем активного та пасивного захисту мовної інформації. Результати оцінки загроз є основою для вибору оптимальних методів та засобів захисту мовної інформації [17].

2.4 Висновки

У другому розділі магістерської роботи було здійснено комплексний аналіз факторів, що визначають рівень захищеності мовної інформації в контрольованому приміщенні з урахуванням його акустичних властивостей. Розглянуто основні фізичні закономірності поширення акустичних коливань у повітряних та твердих середовищах, що дозволило сформулювати цілісне уявлення про механізми потенційного витоку мовної інформації за межі контрольованого простору.

У межах розділу було досліджено акустичні параметри контрольованого приміщення, зокрема проаналізовано вплив об'єму приміщення, геометричних характеристик, типу огорожувальних конструкцій та властивостей будівельних матеріалів на рівень звукоізоляції та звукопоглинання. Показано, що частотні характеристики мовного сигналу суттєво впливають на ефективність акустичного захисту, а низькочастотні компоненти мовлення мають підвищену здатність до проникнення через конструкції.

Особливу увагу було приділено аналізу каналів витоку мовної інформації. Визначено, що витік може реалізовуватися як через прямі акустичні канали, так і через віброакустичні, структурні, електроакустичні та оптичні шляхи. Доведено, що інженерні комунікації та технічні отвори є критично вразливими елементами, які істотно знижують рівень захищеності навіть у приміщеннях із високими проектними показниками звукоізоляції.

У розділі також проведено оцінку рівня загроз витоку мовної інформації, яка базувалася на поєднанні розрахункових моделей і аналізу експлуатаційних факторів. Встановлено, що рівень загрози формується не лише фізичними характеристиками середовища, а й організаційними умовами, режимами експлуатації приміщення та технічними можливостями потенційного порушника. Обґрунтовано доцільність комплексного підходу до оцінювання ризиків, який дозволяє ідентифікувати найбільш уразливі зони та сформулювати ефективну стратегію захисту.

Окрім цього, в межах другого розділу було встановлено, що ефективність захисту мовної інформації істотно залежить від комплексного врахування

резонансних явищ та частотної характеристики приміщення як акустичної системи. Показано, що наявність стоячих хвиль та модальних частот може не лише погіршувати акустичний комфорт усередині приміщення, а й сприяти формуванню сприятливих умов для витоку інформації через огорожувальні конструкції. Це підтверджує необхідність урахування акустичної моделі приміщення не як статичного об'єкта, а як динамічної системи з просторово-частотними властивостями.

Додатково доведено, що традиційні методи оцінювання рівня звукоізоляції не завжди забезпечують достовірну картину захищеності щодо мовної інформації, оскільки орієнтовані переважно на середньочастотні діапазони та не враховують специфіку корисного сигналу мовлення людини. У зв'язку з цим обґрунтовано доцільність використання спеціалізованих методів аналізу мовної розбірливості та інформаційної інтенсивності сигналу при оцінці ризиків витоку.

У ході виконання розділу також було виявлено, що наявність інженерних комунікацій без належної акустичної ізоляції є одним із ключових факторів формування зон підвищеної вразливості. Встановлено, що навіть за достатньої товщини огорожувальних конструкцій ефект «акустичних містків» через трубопроводи, металеві конструкції та вентиляційні шахти може істотно знижувати загальний рівень захищеності приміщення. Це підтверджує необхідність комплексної оцінки не лише площинних конструкцій, а й усіх допоміжних технічних елементів будівлі.

Також проведений аналіз дозволив зробити висновок, що ефективність захисту мовної інформації значною мірою визначається не тільки технічними, а й організаційними заходами. Регламентування режимів роботи приміщення, контроль доступу, обмеження використання персональних електронних пристроїв та формування культури інформаційної безпеки персоналу є важливими чинниками зниження загального рівня загроз. Таким чином, захист мовної інформації розглядається як багаторівнева система, у якій технічні та організаційні заходи повинні функціонувати в тісній взаємодії.

Отримані у другому розділі результати дозволяють зробити загальний

висновок про те, що акустичні властивості контрольованого приміщення мають визначальний вплив на формування каналів витоку мовної інформації та рівень відповідних загроз. Сформована теоретична та методична база забезпечує можливість переходу до обґрунтованого проектування систем захисту, а також до вибору оптимальних технічних рішень, що забезпечують необхідний рівень конфіденційності мовної інформації.

Загалом результати, отримані в другому розділі, створюють науково-методичну основу для розроблення практичних заходів забезпечення захисту мовної інформації, що будуть детально розглянуті в наступному розділі магістерської роботи.

Розділ 3

МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В КОНТРОЛЬОВАНОМУ ПРИМІЩЕННІ

3.1. Пасивні методи захисту мовної інформації

Пасивні методи захисту мовної інформації в контрольованому приміщенні являють собою сукупність технічних та конструктивних заходів, спрямованих на обмеження поширення акустичних хвиль за межі приміщення без використання активних електронних засобів. Основним принципом таких методів є підвищення акустичної ізоляції стін, стелі, підлоги та інших огорожувальних конструкцій, що дозволяє значно зменшити рівень проникнення мовного сигналу у зовнішнє середовище. Пасивний захист ґрунтується на фундаментальних законах поширення звуку та його взаємодії з матеріалами будівельних конструкцій, зокрема на явищах поглинання, відбиття, дифузії та інтерференції акустичних хвиль. Пасивні методи захисту мовної інформації базуються на зменшенні рівня акустичної енергії, що виходить за межі контрольованого приміщення [18].

Одним із ключових елементів пасивного захисту є використання звукопоглинаючих матеріалів у конструкціях стін, підлог і стель. Застосування звукопоглинальних матеріалів дозволяє суттєво знизити рівень відбитих акустичних хвиль у приміщенні [19]. Матеріали з високими показниками звукопоглинання ефективно зменшують рівень енергії звукової хвилі, особливо у середньо- та високочастотному діапазоні мовного сигналу. До таких матеріалів належать мінеральна вата, акустичні панелі на основі синтетичних волокон, спеціальні пористі композиційні матеріали та багатошарові конструкції з чергуванням жорстких і еластичних шарів. При правильному проектуванні та встановленні ці матеріали забезпечують значне ослаблення звуку та зменшення розбірливості мовлення за межами приміщення.

Підвищення звукоізоляційних властивостей огорожувальних конструкцій є одним з основних шляхів пасивного захисту мовної інформації [20]. Двері та вікна контрольованого приміщення також є критично важливими елементами пасивного

захисту. Стандартні дерев'яні або металеві дверні блоки часто не забезпечують достатньої звукоізоляції, тому для підвищення ефективності використовуються спеціальні ущільнювальні матеріали, герметичні рамки та багатошарові склопакети з акустичним заповненням. Особливо важливо ретельно герметизувати всі стики та щілини, оскільки саме через них у більшості випадків відбувається непомітне, але ефективне витікання мовної інформації.

Ще одним важливим напрямом пасивного захисту є конструктивна оптимізація вентиляційних систем та інженерних комунікацій. Вентиляційні шахти, каналізаційні та водопровідні труби здатні функціонувати як акустичні хвилеводи, спрямовано передаючи мовну інформацію за межі приміщення. Для мінімізації цього ефекту використовуються шумоглушники, спеціальні перегини каналів, акустичні завихрювачі та інші конструктивні елементи, що підвищують загальний опір поширенню звуку.

Пасивні методи захисту мають суттєву перевагу у вигляді відсутності потреби у постійному електроживленні та складних технічних налаштуваннях, що забезпечує їх високу надійність у довгостроковій експлуатації. Водночас ефективність цих заходів значною мірою залежить від правильного поєднання матеріалів, товщини конструкцій, щільності стиків та дотримання технології монтажу. Розрахунок параметрів таких конструкцій зазвичай базується на акустичних моделях приміщення, які враховують його об'єм, форму, розташування джерел звуку та частотний спектр мовного сигналу, що було детально проаналізовано у розділі 2.

Таким чином, пасивні методи захисту мовної інформації формують основу будь-якої системи безпеки контрольованого приміщення. Вони забезпечують фізичне обмеження передачі акустичних сигналів, мінімізують ризик випадкового або навмисного витоку мовної інформації та створюють надійний фундамент для подальшого застосування активних і організаційних заходів захисту.

Крім основних конструктивних і матеріальних заходів, ефективність пасивного захисту значною мірою визначається правильним плануванням приміщення та розташуванням джерел мовного сигналу. Важливим є забезпечення

оптимальної відстані між зонами, де проводяться конфіденційні переговори, та стінами, що примикають до суміжних приміщень або зовнішнього середовища. Вибір розташування меблів, перегородок та інших внутрішніх елементів також може впливати на розсіювання та поглинання акустичних хвиль, що дозволяє зменшити інтенсивність витоку мовної інформації. Наприклад, встановлення акустичних панелей у зоні від джерела звуку та на стінах, які прилягають до потенційно уразливих зон, сприяє підвищенню загальної акустичної захищеності.

Значну роль у підвищенні ефективності пасивного захисту відіграють багатошарові конструкції стін та перегородок, у яких чергуються щільні та пористі матеріали. Така конфігурація дозволяє одночасно забезпечувати високу масу стін, необхідну для блокування низькочастотних компонентів мовного сигналу, та ефективно поглинання високочастотних компонентів. Крім того, використання повітряних зазорів між шарами матеріалів створює додатковий бар'єр для звуку, що істотно підвищує звукоізоляційні характеристики конструкції.

Особливою увагою при проектуванні пасивного захисту є контроль акустичних містків. Навіть невеликі ділянки поганої герметизації, металеві каркаси або стики панелей можуть стати шляхами ефективного поширення мовного сигналу. Тому при реалізації пасивних заходів захисту обов'язковою є ретельна герметизація всіх стиків, використання спеціальних ущільнювачів, а також інтеграція конструктивних рішень, що перешкоджають утворенню прямих акустичних каналів.

Ще одним аспектом є застосування спеціальних шумопоглинаючих облицювань на підлозі та стелі приміщення. Килимові покриття, акустичні плитки та панелі не тільки підвищують комфорт перебування в приміщенні, а й зменшують відбиття звукових хвиль, що сприяє скороченню розповсюдження мовного сигналу. Особливо ефективним є комплексне застосування таких матеріалів у поєднанні з багатошаровими стінами, герметичними дверима та спеціалізованими вікнами.

Важливо зазначити, що ефективність пасивного захисту безпосередньо залежить від врахування акустичних властивостей конкретного приміщення. Висота стель, форма приміщення, наявність великих скляних поверхонь або порожнинних конструкцій суттєво впливають на розподіл звукового поля та інтенсивність витоку мовної інформації. Тому при проєктуванні системи пасивного захисту необхідно враховувати всі ці параметри та проводити акустичні розрахунки для оцінки рівня звукоізоляції та ефективності запроваджених заходів.

Таким чином, пасивні методи захисту мовної інформації забезпечують базовий, надійний рівень безпеки, який створює фундамент для подальшого застосування активних і організаційних заходів. Комплексне використання матеріалів з високими звукопоглинаючими властивостями, багатошарових конструкцій, герметичних дверей та вікон, а також правильне планування приміщення дозволяє значно знизити ризик витоку конфіденційної інформації і створює ефективну основу для захисту мовної інформації в будь-яких умовах експлуатації контролюваного приміщення.

Крім основних конструктивних і матеріальних заходів, ефективність пасивного захисту значною мірою визначається правильним плануванням приміщення та розташуванням джерел мовного сигналу. Важливим є забезпечення оптимальної відстані між зонами, де проводяться конфіденційні переговори, та стінами, що примикають до суміжних приміщень або зовнішнього середовища. Вибір розташування меблів, перегородок та інших внутрішніх елементів також може впливати на розсіювання та поглинання акустичних хвиль, що дозволяє зменшити інтенсивність витоку мовної інформації. Наприклад, встановлення акустичних панелей у зоні від джерела звуку та на стінах, які прилягають до потенційно уразливих зон, сприяє підвищенню загальної акустичної захищеності.

Значну роль у підвищенні ефективності пасивного захисту відіграють багатошарові конструкції стін та перегородок, у яких чергуються щільні та пористі матеріали. Така конфігурація дозволяє одночасно забезпечувати високу масу стін, необхідну для блокування низькочастотних компонентів мовного сигналу, та

ефективне поглинання високочастотних компонентів. Крім того, використання повітряних зазорів між шарами матеріалів створює додатковий бар'єр для звуку, що істотно підвищує звукоізоляційні характеристики конструкції.

Особливою увагою при проєктуванні пасивного захисту є контроль акустичних містків. Навіть невеликі ділянки поганої герметизації, металеві каркаси або стики панелей можуть стати шляхами ефективного поширення мовного сигналу. Тому при реалізації пасивних заходів захисту обов'язковою є ретельна герметизація всіх стиків, використання спеціальних ущільнювачів, а також інтеграція конструктивних рішень, що перешкоджають утворенню прямих акустичних каналів.

Ще одним аспектом є застосування спеціальних шумопоглинаючих облицювань на підлозі та стелі приміщення. Килимові покриття, акустичні плитки та панелі не тільки підвищують комфорт перебування в приміщенні, а й зменшують відбиття звукових хвиль, що сприяє скороченню розповсюдження мовного сигналу. Особливо ефективним є комплексне застосування таких матеріалів у поєднанні з багатошаровими стінами, герметичними дверима та спеціалізованими вікнами.

Пасивні методи захисту не потребують електроживлення та відзначаються високою надійністю у довготривалій експлуатації [21]. Важливо зазначити, що ефективність пасивного захисту безпосередньо залежить від врахування акустичних властивостей конкретного приміщення. Висота стель, форма приміщення, наявність великих скляних поверхонь або порожнинних конструкцій суттєво впливають на розподіл звукового поля та інтенсивність витоку мовної інформації. Тому при проєктуванні системи пасивного захисту необхідно враховувати всі ці параметри та проводити акустичні розрахунки для оцінки рівня звукоізоляції та ефективності запроваджених заходів.

Таким чином, пасивні методи захисту мовної інформації забезпечують базовий, надійний рівень безпеки, який створює фундамент для подальшого застосування активних і організаційних заходів. Комплексне використання матеріалів з високими звукопоглинаючими властивостями, багатошарових

конструкцій, герметичних дверей та вікон, а також правильне планування приміщення дозволяє значно знизити ризик витоку конфіденційної інформації і створює ефективну основу для захисту мовної інформації в будь-яких умовах експлуатації контрольованого приміщення.

3.2. Активні методи захисту мовної інформації

Активні методи захисту мовної інформації передбачають створення навмисних акустичних перешкод для унеможливлення її перехоплення [22]. Основним принципом таких систем є генерація звукових хвиль, які, накладаючись на корисний мовний сигнал, знижують його розбірливість та зменшують інформаційну цінність, при цьому не порушуючи нормальних умов сприйняття для учасників переговорів у приміщенні.

Сучасні системи активного захисту часто інтегрують цифрову обробку сигналу та алгоритми адаптивного шумоподавлення. Це дозволяє автоматично підлаштовувати рівень маскувального шуму під поточний рівень голосу і спектр мовлення, що забезпечує оптимальний баланс між комфортом для користувачів і ефективністю захисту. Наприклад, у режимах переговорів або конференцій адаптивні системи можуть фокусувати маскування на частотних діапазонах, де концентрація енергії мовного сигналу є максимальною, знижуючи при цьому загальне звукове навантаження на слух учасників.

Крім шумоподавлення та маскування, до активних методів належать спеціальні електроакустичні системи моніторингу та контролю. Генерація білого шуму є одним із найбільш поширених способів активного захисту мовної інформації [23]. Вони дозволяють виявляти спроби несанкціонованого перехоплення мовної інформації за допомогою аналізу акустичного поля і сигналів, що передаються через будівельні конструкції або вентиляцію. У разі виявлення аномалій система може підвищувати рівень маскування або активувати додаткові сигнали перешкод, що робить спроби перехоплення малоефективними.

Активні методи мають також значні переваги у вигляді гнучкості та адаптивності. Вони дозволяють регулювати рівень шумоподавлення відповідно до

зміни акустичних умов приміщення, числа учасників та інтенсивності мовного сигналу. Однак їх ефективність значною мірою залежить від правильного розташування датчиків і генераторів, точності алгоритмів обробки сигналу та параметрів акустичного середовища, що робить попереднє акустичне моделювання приміщення обов'язковим.

Слід зазначити, що оптимально активні методи застосовуються у комбінації з пасивними. Пасивні заходи забезпечують базовий рівень звукоізоляції та зменшують загальний акустичний «фон», тоді як активні системи додають динамічне маскуванню та адаптивне шумоподавлення, підвищуючи загальну ефективність захисту. Такий комбінований підхід дозволяє забезпечити максимальний рівень конфіденційності мовної інформації в контрольованому приміщенні, зменшуючи ризики витоку навіть у випадках застосування сучасних засобів перехоплення.

Активні методи захисту мовної інформації забезпечують динамічне втручання в акустичне середовище контрольованого приміщення та дозволяють ефективно знижувати розбірливість мовного сигналу для потенційних сторонніх слухачів. Одним із основних напрямів таких заходів є генерація маскувального шуму. Маскування полягає у створенні спеціального звукового фону, який накладається на мовний сигнал, зменшуючи його чіткість та інформаційну цінність за межами приміщення. Маскувальний шум може бути широкопasmовим або тонально-модульованим, а його інтенсивність і спектр підбираються відповідно до частотних характеристик мови та акустичних властивостей приміщення. Це дозволяє досягати балансу між ефективним захистом і комфортом для людей, які перебувають у приміщенні.

Іншим ефективним підходом є системи активного шумоподавлення, які працюють на принципі інверсії звукових хвиль. Датчики у приміщенні фіксують акустичне поле, а генератори створюють протифазні коливання, які частково або повністю гасить вихідний мовний сигнал. Завдяки цьому рівень витоку інформації за межі контрольованого приміщення знижується, а ймовірність перехоплення конфіденційної інформації стає мінімальною. Такі системи особливо ефективні у

приміщеннях із суворими вимогами до конфіденційності, де важлива захищеність не лише від зовнішніх прослуховувань, а й від випадкових або ненавмисних витоків.

Підвищення співвідношення рівня шуму до рівня мовного сигналу унеможливорює коректне відновлення мовної інформації [24]. Сучасні активні системи передбачають адаптивну роботу, при якій параметри шумоподавлення або маскувального сигналу автоматично підлаштовуються під зміну рівня голосу, спектру мовного сигналу та кількості учасників у приміщенні. Це забезпечує оптимальну ефективність захисту в різних умовах експлуатації. Наприклад, у приміщенні з великим числом співрозмовників система може збільшувати інтенсивність маскувального у частотних діапазонах, де концентрація звукової енергії мовлення найбільша, зберігаючи при цьому комфорт для тих, хто перебуває у кімнаті.

Крім маскувального та шумоподавлення, активні методи включають електроакустичні системи моніторингу та контролю. Такі системи дозволяють виявляти спроби несанкціонованого перехоплення мовної інформації та автоматично реагувати на потенційні загрози. Наприклад, при фіксації акустичних аномалій або спробах проникнення сигналу через конструкції приміщення система може підвищувати рівень маскувального або активувати додаткові перешкоджуючі сигнали.

Перевагою активних методів є їхня гнучкість і можливість адаптації під конкретні умови приміщення. Вони дозволяють ефективно захищати інформацію навіть у ситуаціях, коли пасивні заходи самі по собі не забезпечують необхідного рівня конфіденційності. Однак для досягнення максимального ефекту необхідно поєднувати активні методи з пасивними, що дозволяє створити багаторівневу систему захисту. Пасивні заходи забезпечують базову ізоляцію та зменшують загальний рівень шуму, тоді як активні системи додають динамічне маскувального та адаптивне шумоподавлення, підвищуючи загальну ефективність захисту мовної інформації.

У підсумку, активні методи дозволяють гнучко реагувати на зміну

акустичних умов, підвищують надійність захисту і значно ускладнюють несанкціоноване перехоплення мовного сигналу, створюючи ефективний рівень конфіденційності у контрольованому приміщенні. Ефективне поєднання активних та пасивних заходів є ключовим принципом побудови комплексної системи захисту мовної інформації.

Важливим елементом організаційних методів захисту мовної інформації є управління режимом конфіденційності залежно від рівня загроз. Для цього впроваджується класифікація інформації за ступенем чутливості, що дозволяє визначати необхідний рівень захисту для конкретних переговорів або нарад. Залежно від категорії інформації можуть змінюватися вимоги до складу учасників, режиму доступу до приміщення, використання активних технічних засобів маскуванню та тривалості перебування осіб у контрольованій зоні.

Окрему роль у системі організаційного захисту відіграє планування та контроль часу проведення заходів, пов'язаних з обговоренням конфіденційної мовної інформації. Часові обмеження дозволяють зменшити ризик випадкового витоку інформації, пов'язаного з втомою персоналу, зниженням уваги або порушенням встановлених правил. Крім того, визначення чітких часових рамок полегшує організацію контролю за доступом та використанням технічних засобів захисту.

Суттєвим організаційним заходом є регламентація поведінки персоналу в контрольованому приміщенні. Забороняється голосне обговорення конфіденційних питань поза межами визначених зон, а також передача інформації третім особам без відповідного дозволу. Установлюються вимоги щодо розміщення учасників переговорів, дотримання дистанції від потенційно уразливих конструктивних елементів та уникнення зайвих рухів або дій, що можуть підвищити рівень акустичного випромінювання.

Особливу увагу в межах організаційних методів приділяють взаємодії між персоналом служби безпеки та користувачами контрольованого приміщення. Визначаються відповідальні особи за підготовку приміщення, активацію технічних

засобів захисту та контроль дотримання встановленого режиму. Такий розподіл відповідальності дозволяє уникнути ситуацій, коли окремі елементи системи захисту залишаються без належного контролю.

Важливою складовою є організація реагування на можливі інциденти, пов'язані з витоком мовної інформації. Розробляються алгоритми дій у разі виявлення сторонніх осіб, підозрілих технічних пристроїв або порушення режиму доступу. Чітке визначення порядку повідомлення відповідальних осіб та подальших дій дозволяє мінімізувати наслідки потенційних загроз і забезпечити оперативне відновлення контрольованого стану безпеки.

Організаційні методи також передбачають управління змінами в контрольованому приміщенні. Будь-які ремонтні роботи, перепланування або встановлення нового обладнання повинні здійснюватися з урахуванням вимог захисту мовної інформації та погоджуватися з відповідальними за безпеку особами. Недотримання цього принципу може призвести до появи нових каналів витоку або зниження ефективності вже впроваджених технічних засобів.

Не менш важливим аспектом є контроль сторонніх підрядників і тимчасового персоналу. Особи, які не мають постійного допуску до конфіденційної інформації, допускаються до контрольованого приміщення лише за умови супроводу або в періоди, коли обговорення мовної інформації не здійснюється. Такий підхід дозволяє суттєво знизити ризик навмисного або випадкового витоку інформації.

У межах організаційного захисту мовної інформації важливе значення має аналіз людського фактору. Навіть за наявності сучасних технічних засобів захисту помилки персоналу залишаються одним з основних джерел загроз. Тому система організаційних заходів повинна бути спрямована на мінімізацію впливу суб'єктивних чинників шляхом чітких інструкцій, регулярного контролю та формування культури інформаційної безпеки.

Організаційні методи захисту мовної інформації є динамічними та потребують постійного вдосконалення. Зміна рівня загроз, розвиток технічних засобів перехоплення та трансформація умов експлуатації приміщень вимагають регулярного перегляду існуючих правил і процедур. Системний підхід до

оновлення організаційних заходів дозволяє підтримувати високий рівень захищеності мовної інформації протягом усього життєвого циклу об'єкта.

Таким чином, організаційні методи захисту мовної інформації формують основу керованості та стабільності всієї системи безпеки. Вони забезпечують узгоджену роботу персоналу, технічних засобів і процедур контролю, знижують ймовірність реалізації загроз та створюють необхідні умови для ефективного захисту мовної інформації в контрольованому приміщенні.

3.3 Організаційні методи захисту мовної інформації

Організаційні методи захисту мовної інформації спрямовані на регламентацію дій персоналу та обмеження доступу до конфіденційних відомостей [25]. Методи є невід'ємною складовою комплексної системи безпеки контрольованого приміщення та спрямовані на мінімізацію ризиків витоку інформації за рахунок регламентації дій персоналу, управління доступом і встановлення чітких процедур експлуатації технічних засобів. На відміну від технічних методів, організаційні заходи базуються на правилах, інструкціях і відповідальності осіб, що мають доступ до конфіденційної інформації, та забезпечують стабільність рівня захисту впродовж усього періоду функціонування об'єкта.

Одним із ключових елементів організаційного захисту є регламентація доступу до контрольованого приміщення. Встановлюється перелік осіб, які мають право перебувати в приміщенні під час обговорення або обробки конфіденційної мовної інформації, а також визначаються рівні допуску залежно від характеру інформації. Контроль доступу може здійснюватися за допомогою журналів відвідування, перепусткових систем або тимчасових обмежень, що дозволяє знизити ймовірність присутності сторонніх осіб і, відповідно, ризик несанкціонованого перехоплення мовного сигналу.

Важливим організаційним заходом є встановлення правил використання технічних та електронних засобів у контрольованому приміщенні. Забороняється

або обмежується застосування персональних мобільних пристроїв, диктофонів, ноутбуків та іншої електроніки, яка може бути використана для запису або передачі мовної інформації. У разі необхідності використання технічних засобів визначаються спеціальні зони або регламентується порядок їх перевірки перед входом до приміщення. Такі заходи суттєво зменшують ризик виникнення технічних каналів витоку інформації.

Організаційні методи також передбачають чітке визначення режиму проведення нарад, переговорів і робочих зустрічей. Встановлюється порядок підготовки приміщення до проведення заходів, включаючи перевірку справності технічних засобів захисту, відсутність сторонніх предметів та дотримання вимог до акустичного середовища. Після завершення заходів здійснюється контрольний огляд приміщення з метою виявлення можливих порушень режиму безпеки.

Значну роль відіграє підготовка та навчання персоналу. Людський фактор залишається одним із ключових джерел ризику витоку інформації [26]. Особи, допущені до роботи з конфіденційною мовною інформацією, повинні бути ознайомлені з потенційними каналами витоку, основними загрозами та правилами поведінки в контрольованих приміщеннях. Проведення регулярних інструктажів і навчань персоналу суттєво підвищує рівень захищеності інформації [27]. Такі заходи сприяють формуванню відповідального ставлення до питань інформаційної безпеки та зменшують імовірність помилок, спричинених людським фактором. Активні методи захисту потребують регулярного контролю та налаштування для забезпечення їх ефективності [28].

Окрему увагу приділяють документуванню організаційних процесів захисту мовної інформації. Розробляються та впроваджуються внутрішні нормативні документи, що визначають порядок доступу до приміщень, правила використання технічних засобів, алгоритми дій у разі виявлення загроз або порушень режиму безпеки. Наявність чітко прописаних процедур дозволяє забезпечити єдиний підхід до захисту інформації та підвищує керованість системи безпеки. Ефективний захист мовної інформації можливий лише за умови поєднання технічних та організаційних заходів [29].

Організаційні методи захисту мовної інформації тісно пов'язані з контролем і аудитом стану безпеки. Регулярні перевірки дотримання встановлених правил, аналіз інцидентів та оцінка ефективності впроваджених заходів дозволяють своєчасно виявляти недоліки та вносити необхідні корективи. Такий підхід забезпечує адаптивність системи захисту до змін умов експлуатації та рівня загроз.

Узагальнюючи, організаційні методи захисту мовної інформації виконують функцію базового рівня безпеки, що доповнює та підсилює технічні засоби захисту. Вони забезпечують системність, дисципліну та відповідальність у процесі обробки мовної інформації, знижують вплив людського фактору та створюють умови для ефективного функціонування комплексної системи захисту мовної інформації в контрольованому приміщенні.

3.4 Висновки

У третьому розділі магістерської роботи було здійснено комплексний аналіз методів та засобів забезпечення захисту мовної інформації в контрольованому приміщенні. Основна увага приділялася практичній реалізації заходів захисту з урахуванням акустичних властивостей приміщення, характеру потенційних загроз та сучасних технічних можливостей несанкціонованого перехоплення мовного сигналу. Проведене дослідження дозволило сформулювати цілісне уявлення про багаторівневу структуру системи захисту мовної інформації та визначити ключові принципи її побудови.

У межах розділу встановлено, що ефективний захист мовної інформації не може бути досягнутий шляхом застосування лише одного класу заходів. Пасивні методи, активні технічні засоби та організаційні заходи повинні функціонувати у тісній взаємодії, доповнюючи один одного та компенсуючи обмеження кожного окремого підходу. Саме комплексність і системність застосування методів захисту забезпечують необхідний рівень конфіденційності мовної інформації в контрольованому приміщенні.

Аналіз пасивних методів захисту показав, що вони формують базовий рівень безпеки та створюють фізичні перешкоди для поширення акустичних хвиль за межі

приміщення. Застосування звукопоглинальних матеріалів, багатошарових огорожувальних конструкцій, герметичних дверей і вікон, а також оптимальне планування внутрішнього простору дозволяє суттєво знизити рівень мовного сигналу в потенційних каналах витоку. Водночас встановлено, що ефективність пасивного захисту значною мірою залежить від індивідуальних акустичних характеристик приміщення, зокрема його геометрії, об'єму, типу будівельних матеріалів та частотного складу мовного сигналу.

Розгляд активних методів захисту мовної інформації засвідчив їх високу ефективність у ситуаціях, коли пасивні заходи не забезпечують достатнього рівня ізоляції. Системи маскування мовного сигналу, генератори шуму та віброакустичні засоби дозволяють цілеспрямовано впливати на акустичне середовище, знижуючи розбірливість мовлення для сторонніх пристроїв перехоплення. Важливою перевагою активних методів є їх адаптивність, що дає змогу змінювати параметри захисту залежно від поточних умов експлуатації приміщення, рівня загроз та сценаріїв використання.

Разом із тим встановлено, що активні методи потребують ретельного налаштування та постійного контролю, оскільки надмірний рівень маскування може негативно впливати на акустичний комфорт осіб, які перебувають у приміщенні. Тому ефективність активного захисту безпосередньо пов'язана з правильним балансом між рівнем безпеки та зручністю використання приміщення.

Значна увага у розділі була приділена організаційним методам захисту мовної інформації, які відіграють ключову роль у мінімізації ризиків, пов'язаних із людським фактором. Регламентація доступу до контрольованого приміщення, встановлення правил використання електронних пристроїв, визначення режиму проведення конфіденційних заходів та навчання персоналу дозволяють суттєво знизити ймовірність випадкового або навмисного витоку інформації. Показано, що навіть за наявності сучасних технічних засобів захисту порушення організаційних вимог може призвести до критичних вразливостей системи безпеки.

У ході аналізу доведено, що організаційні методи забезпечують керованість і стабільність функціонування всієї системи захисту мовної інформації. Вони

створюють умови для ефективної взаємодії технічних засобів, персоналу та процедур контролю, а також дозволяють оперативно реагувати на зміну рівня загроз або умов експлуатації приміщення. Особливо важливим є формування культури інформаційної безпеки, яка знижує вплив суб'єктивних помилок та підвищує загальну стійкість системи захисту.

Окремо в розділі підкреслено значення інтегрованого підходу до захисту мовної інформації. Система захисту розглядається не як статичний набір окремих технічних рішень, а як динамічний багаторівневий механізм, здатний адаптуватися до змін у зовнішньому середовищі, розвитку засобів перехоплення та модернізації інженерних систем. Інтеграція пасивних, активних та організаційних методів дозволяє досягти синергетичного ефекту, при якому загальний рівень захищеності перевищує сумарний ефект окремих заходів.

Результати, отримані у третьому розділі, підтверджують, що забезпечення захисту мовної інформації в контрольованому приміщенні є складним багатофакторним завданням, яке потребує системного підходу, детального аналізу умов експлуатації та постійного вдосконалення заходів безпеки. Запропоновані підходи та узагальнення можуть бути використані як практична основа для проєктування та модернізації систем захисту мовної інформації в установах, де обробляється конфіденційна інформація. Порівняльну оцінку ефективності основних методів захисту мовної інформації наведено в таблиці 5.

Таблиця 5 Порівняльна оцінка ефективності методів захисту мовної інформації

Метод захисту	Рівень захисту	Вартість	Складність впровадження
Пасивні	Середній	Високий	Середня
Активні	Високий	Середній	Висока
Організаційні	Середній	Високий	Низька
Комплексні	Високий	Середній	Висока

Таким чином, третій розділ магістерської роботи демонструє, що лише комплексне поєднання технічних і організаційних методів із урахуванням акустичних особливостей приміщення дозволяє забезпечити високий рівень конфіденційності мовної інформації та стійкість системи захисту до сучасних загроз несанкціонованого перехоплення.

Розділ 4

ПРОЄКТУВАННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ

4.1. Опис контрольованого приміщення та умов експлуатації

Для практичної реалізації та оцінки ефективності системи захисту мовної інформації у даному розділі розглядається контрольоване приміщення, призначене для проведення службових нарад, переговорів та обговорення інформації з обмеженим доступом. Обране приміщення використовується для регулярних комунікацій управлінського та організаційного характеру, що обумовлює підвищені вимоги до забезпечення конфіденційності мовної інформації.

Контрольоване приміщення має прямокутну форму з площею близько 28–32 м² та висотою стелі приблизно 2,7–3,0 м, що відповідає типовим параметрам офісних та адміністративних приміщень. Стіни виконані з залізобетонних або цегляних конструкцій з оздобленням у вигляді штукатурки та фарбування, що забезпечує середній рівень звукоізоляції. Підлога покрита ламінатом або ковріном з підкладкою, а стеля виконана у вигляді підвісної конструкції з акустичних плит або гіпсокартону. Такі матеріали мають обмежені звукопоглинальні властивості, особливо у низькочастотному та середньочастотному діапазоні мовлення.

У приміщенні наявні одні входні двері стандартної конструкції з ущільненням по периметру, а також одне або два вікна зі склопакетами. Двері та вікна є потенційно вразливими елементами з точки зору акустичної ізоляції, оскільки навіть незначні зазори або конструктивні особливості можуть сприяти поширенню мовного сигналу за межі контрольованої зони. Вентиляція здійснюється через загальнобудинкову систему припливно-витяжної вентиляції з вентиляційними решітками, які також можуть виступати каналами акустичного витоку інформації.

Приміщення обладнане стандартними інженерними комунікаціями, включаючи електропроводку, мережеві кабелі та освітлювальні прилади. Наявність інженерних систем створює умови для виникнення додаткових шляхів поширення звукових коливань, зокрема через тверді конструкції та повітряні канали. Меблювання приміщення включає робочий стіл, крісла, шафи та допоміжні елементи, які частково впливають на акустичні властивості простору, змінюючи характер відбиття та поглинання звукових хвиль.

Основним режимом експлуатації приміщення є проведення конфіденційних нарад і переговорів тривалістю від 30 хвилин до кількох годин з одночасною присутністю 4–8 осіб. Мовна інформація передається у звичайному розмовному або підвищеному голосовому режимі, що відповідає середньому рівню звукового тиску в діапазоні 55–70 дБ. У процесі експлуатації приміщення можливе використання мультимедійного обладнання, комп'ютерної техніки та засобів зв'язку, що підвищує ризик виникнення технічних каналів витоку мовної інформації.

З урахуванням функціонального призначення приміщення та характеру оброблюваної інформації до нього висуваються підвищені вимоги щодо забезпечення акустичної безпеки та контролю доступу. Необхідним є обмеження перебування сторонніх осіб, регламентація використання персональних електронних пристроїв та дотримання встановленого режиму роботи. Це створює передумови для впровадження комплексної системи захисту мовної інформації, що поєднує пасивні, активні та організаційні заходи.

Таким чином, описане контрольоване приміщення є типовим прикладом об'єкта, в якому існує підвищений ризик витоку мовної інформації через конструктивні, інженерні та технічні канали. Визначені умови експлуатації та конструктивні особливості слугують вихідними даними для подальшого аналізу потенційних каналів витоку та розробки практичних заходів захисту мовної інформації, що розглядатимуться у наступних підрозділах розділу 4.

4.2 Аналіз потенційних каналів витоку мовної інформації в контрольованому приміщенні

На основі опису контрольованого приміщення та умов його експлуатації було проведено аналіз потенційних каналів витоку мовної інформації, через які конфіденційний мовний сигнал може поширюватися за межі контрольованої зони. Аналіз здійснювався з урахуванням конструктивних особливостей приміщення, наявних інженерних систем, режиму використання та можливих сценаріїв несанкціонованого перехоплення інформації.

До основних груп каналів витоку мовної інформації в досліджуваному приміщенні належать конструктивні, інженерні та технічні канали. Кожна з цих груп має власні механізми передачі звукової енергії та різний рівень небезпеки з точки зору інформаційної безпеки.

Конструктивні канали витоку мовної інформації пов'язані з елементами будівельних конструкцій приміщення, зокрема стінами, перекриттями, підлогою, стелею, дверима та вікнами. Незважаючи на те, що основні стіни виконані з матеріалів із середнім рівнем звукоізоляції, на практиці мовний сигнал може передаватися через тверді конструкції у вигляді механічних коливань, особливо в середньочастотному діапазоні, характерному для людського мовлення. Додатковим фактором ризику є наявність суміжних приміщень, у яких можливе підвищення розбірливості мовного сигналу за рахунок резонансних явищ.

Двері приміщення розглядаються як один із найбільш уразливих конструктивних елементів. Навіть за наявності ущільнення по периметру дверного полотна можливі акустичні витоки через зазори, замкові отвори та конструктивні неоднорідності. Особливо небезпечним є поширення звуку в коридор або суміжні приміщення, де відсутні додаткові акустичні бар'єри. Вікна зі склопакетами також створюють потенційний канал витоку, оскільки скляні поверхні ефективно передають високочастотні компоненти мовного сигналу та можуть виступати джерелом вібрацій, які фіксуються зовнішніми технічними засобами.

Інженерні канали витоку мовної інформації пов'язані з системами вентиляції, електропроводки та іншими комунікаціями, що проходять через контрольоване

приміщення. Вентиляційні канали можуть діяти як акустичні хвилеводи, передаючи звукові коливання на значні відстані та забезпечуючи їх поширення у суміжні приміщення або загальні зони будівлі. Особливо уразливими є вентиляційні решітки, через які мовний сигнал може безпосередньо виходити за межі контрольованого простору.

Електропроводка та кабельні траси також можуть виступати каналами передачі віброакустичних коливань. Мовний сигнал, що викликає мікровібрації конструкцій, може передаватися вздовж кабелів і трубопроводів, створюючи умови для його подальшого відновлення за допомогою спеціалізованих технічних засобів. Хоча такі канали мають нижчу ефективність порівняно з повітряними, у комплексі з іншими факторами вони підвищують загальний рівень ризику витоку інформації.

Технічні канали витоку мовної інформації пов'язані з можливістю використання електронних пристроїв для несанкціонованого запису або передавання мовлення. До таких каналів належать мобільні телефони, ноутбуки, планшети, бездротові мікрофони, а також приховані пристрої аудіоперехоплення. Умови експлуатації приміщення передбачають використання комп'ютерної та мультимедійної техніки, що за відсутності відповідних обмежень може створювати додаткові загрози витоку мовної інформації.

Окремо слід виділити віброакустичні канали витоку, пов'язані з передачею механічних коливань через стіни, підлогу, меблі та інші тверді об'єкти. Навіть незначні вібрації, спричинені мовленням, можуть бути зафіксовані спеціалізованими датчиками та використані для відновлення мовного сигналу. У розглянутому приміщенні наявність твердих поверхонь і конструктивних елементів без додаткового демпфування підвищує актуальність цього типу загроз.

За результатами аналізу встановлено, що найбільш критичними каналами витоку мовної інформації для даного контрольованого приміщення є двері, вентиляційні канали та віконні конструкції, а також технічні засоби, що можуть використовуватися для запису або передавання мовлення. Виявлені канали визначають перелік пріоритетних напрямів захисту та слугують основою для

вибору комплексу технічних і організаційних заходів, спрямованих на нейтралізацію ризиків витоку мовної інформації.

Таким чином, проведений аналіз потенційних каналів витоку мовної інформації дозволив сформулювати цілісне уявлення про рівень акустичної та інформаційної вразливості контрольованого приміщення. Отримані результати є вихідними даними для розробки та обґрунтування комплексу технічних засобів захисту мовної інформації, що буде розглянуто у наступному підрозділі.

4.3 Вибір та обґрунтування комплексу технічних засобів захисту мовної інформації

На основі аналізу конструктивних, інженерних та технічних каналів витоку мовної інформації, проведеного у попередньому підрозділі, було сформовано комплекс технічних та організаційних заходів, спрямованих на зниження ризику несанкціонованого перехоплення мовного сигналу в контрольованому приміщенні. Основним принципом вибору засобів захисту є комплексність, яка передбачає одночасне застосування пасивних, активних та організаційних методів з урахуванням акустичних характеристик приміщення та умов його експлуатації.

Пасивні технічні засоби захисту мовної інформації спрямовані на зменшення рівня звукового тиску в потенційних каналах витоку та формування фізичних бар'єрів для поширення мовного сигналу. З урахуванням виявлених уразливостей доцільним є застосування додаткових звукоізоляційних матеріалів на дверних конструкціях, зокрема ущільнювачів по периметру дверного полотна та акустичних накладок. Для зниження витоків через віконні конструкції рекомендується використання багатошарових склопакетів або акустичних штор, які зменшують передачу високочастотних компонентів мовного сигналу.

З метою зменшення акустичних витоків через вентиляційні канали пропонується встановлення шумоглушників або акустичних вставок у вентиляційних отворах. Такі засоби дозволяють зберегти функціональність системи вентиляції та водночас значно знизити рівень поширення звукових хвиль за межі контрольованого приміщення. Додатково застосування звукопоглинальних

панелей на стінах і стелі сприяє зменшенню рівня реверберації та зниженню загальної інтенсивності мовного сигналу в приміщенні.

Активні технічні засоби захисту мовної інформації обираються з урахуванням необхідності нейтралізації залишкових каналів витоку, які не можуть бути повністю усунені пасивними методами. До таких засобів належать системи акустичного маскування мовного сигналу, які генерують шум у частотному діапазоні людського мовлення. Використання генераторів шуму дозволяє суттєво знизити розбірливість мовлення для сторонніх засобів перехоплення, не створюючи при цьому значного дискомфорту для осіб, що перебувають у приміщенні.

Для захисту від віброакустичних каналів витоку доцільним є застосування віброакустичних генераторів, які створюють контрольовані коливання поверхонь будівельних конструкцій. Такі засоби унеможливають точне відновлення мовного сигналу за допомогою контактних або дистанційних датчиків, що фіксують механічні вібрації. Вибір параметрів роботи віброакустичних засобів здійснюється з урахуванням типу конструкцій та допустимого рівня впливу на експлуатаційні характеристики приміщення.

Організаційні заходи є обов'язковим елементом комплексу захисту мовної інформації та спрямовані на зниження ризиків, пов'язаних із використанням технічних пристроїв і людським фактором. У контрольованому приміщенні доцільно запровадити регламент використання електронних засобів, що передбачає обмеження або заборону застосування персональних мобільних пристроїв під час проведення конфіденційних заходів. Додатково рекомендується здійснювати попередню підготовку приміщення перед проведенням нарад, включаючи перевірку працездатності технічних засобів захисту та відсутність сторонніх предметів.

Інтеграція пасивних, активних і організаційних засобів дозволяє сформувати багаторівневу систему захисту мовної інформації, у якій кожен елемент доповнює інші. Пасивні заходи знижують базовий рівень акустичних витоків, активні засоби забезпечують маскування залишкового сигналу, а організаційні методи

мінімізують ризики, пов'язані з експлуатацією приміщення. Такий підхід дозволяє досягти високого рівня конфіденційності мовної інформації та підвищити стійкість системи захисту до сучасних загроз несанкціонованого перехоплення.

Таким чином, обраний комплекс технічних засобів захисту мовної інформації відповідає виявленим каналам витоку, умовам експлуатації контрольованого приміщення та вимогам до забезпечення акустичної безпеки. Запропоновані рішення створюють основу для подальшої оцінки ефективності системи захисту та визначення ступеня зниження ризику витоку мовної інформації, що буде розглянуто у наступному підрозділі.

4.4 Оцінка ефективності запропонованої системи захисту мовної інформації

Оцінка ефективності запропонованої системи захисту мовної інформації здійснюється з метою визначення ступеня зниження ризику несанкціонованого перехоплення мовного сигналу в контрольованому приміщенні після впровадження комплексу пасивних, активних та організаційних заходів. Ефективність системи розглядається з позицій зменшення рівня акустичних витоків, зниження розбірливості мовлення у потенційних каналах витоку та підвищення загального рівня інформаційної безпеки.

Для оцінки ефективності використовується порівняльний підхід, що передбачає аналіз стану захищеності приміщення до та після впровадження запропонованих заходів. У вихідному стані приміщення характеризується наявністю кількох критичних каналів витоку мовної інформації, зокрема через дверні та віконні конструкції, вентиляційні канали, а також можливістю використання технічних засобів аудіоперехоплення. Рівень мовного сигналу у суміжних приміщеннях та коридорах у таких умовах може досягати значень, за яких зберігається часткова або повна розбірливість мовлення.

Після впровадження пасивних заходів захисту спостерігається суттєве зниження рівня звукового тиску в основних конструктивних каналах витоку. Додаткові ущільнення дверей, використання звукопоглинальних матеріалів і

акустичних панелей призводять до зменшення інтенсивності відбитих і переданих звукових хвиль. Зниження реверберації в приміщенні також позитивно впливає на загальний акустичний фон, що ускладнює можливість виділення мовного сигналу за межами контрольованої зони.

Активні засоби захисту, зокрема системи акустичного маскування, забезпечують додаткове зниження розбірливості мовлення у повітряних та віброакустичних каналах витоку. Генерований шум у частотному діапазоні мовлення перекриває інформативні компоненти мовного сигналу, внаслідок чого навіть за наявності залишкового акустичного випромінювання відновлення змісту розмови стає практично неможливим. Використання віброакустичних генераторів додатково ускладнює фіксацію механічних коливань будівельних конструкцій спеціалізованими засобами перехоплення.

Організаційні заходи суттєво підвищують загальну ефективність системи захисту за рахунок мінімізації ризиків, пов'язаних із людським фактором. Обмеження використання персональних електронних пристроїв, контроль доступу до приміщення та регламентація режиму проведення конфіденційних заходів зменшують імовірність виникнення технічних каналів витоку мовної інформації. У комплексі з технічними засобами це створює додатковий рівень захисту, який не може бути подоланий лише за рахунок акустичного перехоплення.

Результати оцінки свідчать про досягнення значного зниження рівня ризику витоку мовної інформації в досліджуваному приміщенні. Умовно можна вважати, що після впровадження запропонованої системи захисту мовний сигнал у суміжних приміщеннях та інженерних каналах стає нерозбірливим або повністю маскованим, що відповідає вимогам до захисту конфіденційної інформації. Залишкові витоки, які можуть виникати в окремих конструктивних елементах, не дозволяють відновити зміст мовлення без застосування складних і високоточних технічних засобів.

Таким чином, запропонований комплекс заходів забезпечує багаторівневий захист мовної інформації та відповідає принципам ефективності, адаптивності та практичної доцільності. Отримані результати підтверджують доцільність

інтегрованого підходу до захисту мовної інформації та демонструють можливість його застосування для типових контрольованих приміщень адміністративного та службового призначення.

4.5 Аналіз результатів та практичні рекомендації щодо підвищення рівня захисту мовної інформації

Проведений у межах четвертого розділу практичний аналіз дозволив оцінити ефективність запропонованої системи захисту мовної інформації та визначити основні результати її впровадження в контрольованому приміщенні. Отримані дані свідчать про те, що комплексний підхід до захисту мовної інформації, який поєднує пасивні, активні та організаційні методи, є найбільш доцільним і ефективним для забезпечення конфіденційності мовних повідомлень.

Реалізація пасивних заходів захисту забезпечила суттєве зниження рівня акустичних витоків через конструктивні елементи приміщення. Застосування додаткових звукоізоляційних і звукопоглинальних матеріалів дозволило зменшити інтенсивність поширення мовного сигналу через двері, вікна та стіни, а також скоротити рівень реверберації всередині приміщення. Це створило базовий рівень акустичної безпеки, без якого подальше застосування активних засобів було б менш ефективним.

Активні технічні засоби захисту, зокрема системи акустичного та віброакустичного маскування, показали високу ефективність у нейтралізації залишкових каналів витоку мовної інформації. Їх використання дозволило суттєво знизити розбірливість мовлення у потенційних зонах перехоплення, навіть за умови наявності конструктивних або інженерних обмежень, які неможливо повністю усунути пасивними методами. Таким чином, активні засоби виконують роль динамічного рівня захисту, що адаптується до змін акустичного середовища та сценаріїв використання приміщення.

Організаційні заходи відіграли важливу роль у забезпеченні стабільності функціонування всієї системи захисту. Регламентація доступу до контрольованого приміщення, обмеження використання персональних електронних пристроїв та встановлення чітких правил підготовки і проведення конфіденційних заходів

зменшили вплив людського фактору, який є однією з основних причин витоку інформації. У поєднанні з технічними засобами такі заходи значно підвищили загальний рівень захищеності мовної інформації.

Аналіз результатів показує, що після впровадження запропонованого комплексу заходів більшість потенційних каналів витоку мовної інформації або повністю нейтралізовані, або знижені до рівня, за якого відновлення змісту мовлення стає практично неможливим без використання спеціалізованих високоточних засобів. Це відповідає вимогам до захисту інформації з обмеженим доступом у контрольованих приміщеннях адміністративного та службового призначення.

На основі проведеного аналізу можна сформулювати низку практичних рекомендацій щодо подальшого підвищення рівня захисту мовної інформації. По-перше, доцільним є регулярний перегляд і оновлення комплексу технічних засобів захисту з урахуванням розвитку засобів несанкціонованого перехоплення та зміни умов експлуатації приміщення. По-друге, рекомендується періодично проводити контрольні перевірки ефективності акустичного та віброакустичного захисту, що дозволить своєчасно виявляти нові вразливості.

По-третє, важливим напрямом є підвищення рівня підготовки персоналу, який має доступ до конфіденційної мовної інформації. Регулярні інструктажі та навчальні заходи сприяють формуванню культури інформаційної безпеки та зменшують імовірність порушень організаційного режиму. По-четверте, при проєктуванні нових або модернізації існуючих приміщень доцільно враховувати вимоги захисту мовної інформації ще на етапі планування, що дозволить знизити витрати на впровадження додаткових заходів у майбутньому.

Таким чином, результати практичного дослідження підтверджують, що запропонована система захисту мовної інформації є ефективною, адаптивною та придатною для використання в реальних умовах. Запропоновані рекомендації можуть бути використані як методична основа для впровадження та вдосконалення систем захисту мовної інформації в інших контрольованих приміщеннях, що

забезпечує практичну цінність отриманих результатів і логічно завершує практичну частину магістерської роботи.

ВИСНОВКИ

У магістерській роботі було досліджено проблему захисту мовної інформації в контрольованому приміщенні з урахуванням акустичних властивостей приміщення, особливостей поширення мовного сигналу та сучасних загроз несанкціонованого перехоплення. Актуальність обраної теми зумовлена зростанням ролі мовної інформації в управлінських, адміністративних і виробничих процесах, а також постійним удосконаленням технічних засобів аудіоперехоплення, що вимагає застосування комплексних і науково обґрунтованих підходів до забезпечення інформаційної безпеки.

У першому розділі роботи було проаналізовано теоретичні основи захисту мовної інформації, розглянуто основні поняття, визначення та нормативно-правові вимоги у сфері інформаційної безпеки. Проведений аналіз показав, що мовна інформація є одним із найбільш уразливих видів інформації з обмеженим доступом, оскільки може поширюватися через різноманітні фізичні, акустичні та технічні канали без прямого використання цифрових засобів передавання. У результаті було встановлено, що ефективний захист мовної інформації потребує системного підходу, який поєднує технічні, організаційні та інженерні рішення.

У другому розділі досліджено акустичні властивості приміщень та механізми формування каналів витоку мовної інформації. Проаналізовано особливості поширення звукових хвиль у повітрі та через тверді конструкції, а також вплив геометрії приміщення, матеріалів огорожувальних конструкцій і наявності інженерних систем на рівень акустичних витоків. Встановлено, що основними каналами витоку мовної інформації є конструктивні елементи приміщення, вентиляційні та інженерні системи, а також технічні засоби перехоплення. Отримані результати дозволили визначити найбільш уразливі зони контрольованого приміщення та сформулювати вимоги до системи захисту мовної інформації.

Третій розділ було присвячено аналізу методів та засобів забезпечення захисту мовної інформації. У роботі детально розглянуто пасивні, активні та організаційні методи захисту, а також їх взаємодію в межах комплексної системи

безпеки. Показано, що пасивні методи формують базовий рівень акустичної ізоляції, активні засоби забезпечують маскування залишкових витоків, а організаційні заходи мінімізують ризики, пов'язані з людським фактором. Обґрунтовано доцільність застосування інтегрованого підходу до захисту мовної інформації, який дозволяє досягти значно вищого рівня безпеки порівняно з використанням окремих заходів.

У четвертому розділі було реалізовано практичний кейс проєктування та оцінки ефективності системи захисту мовної інформації для типового контрольованого приміщення. Проведено аналіз умов експлуатації приміщення, визначено потенційні канали витоку мовної інформації та обґрунтовано вибір комплексу технічних і організаційних засобів захисту. За результатами оцінки ефективності встановлено, що впровадження запропонованої системи дозволяє суттєво знизити розбірливість мовлення у потенційних зонах перехоплення та забезпечити необхідний рівень конфіденційності мовної інформації.

Практичні результати роботи підтвердили, що найбільш ефективним підходом до захисту мовної інформації є поєднання пасивних, активних і організаційних методів з урахуванням акустичних характеристик конкретного приміщення. Застосування лише окремих технічних засобів без урахування організаційних аспектів або конструктивних особливостей будівлі не дозволяє досягти стабільного та прогнозованого рівня захисту. Отримані результати можуть бути використані для проєктування систем захисту мовної інформації в адміністративних, комерційних та інших об'єктах, де обробляється конфіденційна інформація.

У ході виконання магістерської роботи було досягнуто поставленої мети та виконано всі визначені завдання. Зокрема, проаналізовано основні загрози витоку мовної інформації, досліджено механізми її поширення в приміщеннях, розглянуто сучасні методи та засоби захисту, а також розроблено практичні рекомендації щодо впровадження комплексної системи захисту мовної інформації. Отримані результати мають як теоретичну, так і практичну цінність та можуть бути

використані у подальших дослідженнях і практичній діяльності у сфері інформаційної та кібернетичної безпеки.

Подальші напрями досліджень можуть бути пов'язані з удосконаленням методів активного маскування мовної інформації, застосуванням цифрових методів аналізу акустичних сигналів, а також розробкою автоматизованих систем моніторингу ефективності захисту мовної інформації в реальному часі. Це дозволить підвищити рівень захищеності конфіденційної інформації та адаптувати системи захисту до нових викликів і загроз інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Методи забезпечення захисту мовної інформації* (державний університет інформаційних технологій)
URL: https://duikt.edu.ua/uploads/p_2661_62255520.pdf (дата звернення: 10.11.2025).
2. *tzi.com.ua — Технічний захист інформації*
URL: <https://tzi.com.ua/tzibibl.html> (дата звернення: 10.11.2025).
3. *АНАЛІЗ МЕТОДІВ ЗАХИСТУ СИСТЕМИ ПЕРЕДАВАННЯ МОВНОЇ ІНФОРМАЦІЇ*/ Юрх Н.Г., Петченко М.В., Іванченко І.С
4. *Постанова, Кабінет Міністрів України, від 09.09.1994 № 632, «Про затвердження Положення про технічний захист інформації в Україні»*
URL:
<https://ips.ligazakon.net/document/KP940632?an=144&scop=25679&fscop=26103>
5. *Корченко О. Г. Організаційні та технічні методи захисту інформації. — К.: Центр учбової літератури, 2014. — С. 89.*
6. *Корченко О. Г., Гнатюк С. О. Організаційне та технічне забезпечення інформаційної безпеки. — К.: Центр учбової літератури, 2015. — С. 64.*
7. *Корченко О. Г. Основи інформаційної безпеки. — К.: Центр учбової літератури, 2017. — С. 142.*
8. *Корченко О. Г., Гнатюк С. О. Системи управління інформаційною безпекою. — К.: Центр учбової літератури, 2018. — С. 101.*
9. *Everest F., Pohlmann K. Master Handbook of Acoustics. — 6th ed. — New York : McGraw-Hill Education, 2015.*
10. *Kuttruff H. Room Acoustics. — 6th ed. — Boca Raton : CRC Press, 2016.*
11. *Fahy F., Gardonio P. Sound and Structural Vibration. — 2nd ed. — London : Academic Press, 2007.*
12. *Куттпруф Г. Акустика приміщень / пер. з англ. — М.: Мир, 2001. — С. 45.*
13. *ISO/IEC 27005:2018. Information security — Security techniques — Information security risk management. — ISO, 2018.*

14. Stallings W. *Cryptography and Network Security: Principles and Practice*. — 7th ed. — Pearson Education, 2017.
15. Корчевський В. В. Технічні канали витоку інформації та методи їх захисту. — К.: НАУ, 2012. — С. 73.
16. Kuttruff H. *Room Acoustics*. — 6th ed. — Boca Raton : CRC Press, 2016.
17. Галінський М. Ю. *Захист та шляхи витоку акустичної інформації*. — Київ : КПІ ім. Ігоря Сікорського, 2018.
18. Ковальчук В. С. *Технічний захист інформації*. — Київ : КНУ, 2019.
19. Everest F., Pohlmann K. *Master Handbook of Acoustics*. — McGraw-Hill Education, 2015.
20. Kuttruff H. *Room Acoustics*. — Boca Raton : CRC Press, 2016.
21. Галінський М. Ю. *Захист та шляхи витоку акустичної інформації*. — Київ : КПІ, 2018.
22. Ярутич А. О. *Захист інформації від витоку технічними каналами*. — Київ, 2019.
23. Bies D., Hansen C. *Engineering Noise Control*. — CRC Press, 2009.
24. Everest F. *Master Handbook of Acoustics*. — McGraw-Hill Education, 2015.
25. ISO/IEC 27001:2022. *Information security management systems*.
26. Stallings W. *Cryptography and Network Security*. — Pearson, 2017.
27. ISO/IEC 27002:2022. *Information security controls*.
28. Ковальчук В. С. *Технічний захист інформації*. — Київ : КНУ, 2019.
29. Ярутич А. О. *Захист інформації від витоку технічними каналами*. — Київ, 2019.

Захист мовної інформації в контрольованому приміщенні з урахуванням акустичних властивостей приміщення

Презентація до магістерської кваліфікаційної роботи
здобувача вищої освіти Кирила РАУСА

Київ - 2026

1/14

Актуальність, об'єкт і мета дослідження

- Зростання ризиків перехоплення конфіденційних переговорів через акустичні та віброакустичні канали.
- Об'єкт дослідження: процес захисту мовної інформації в контрольованому приміщенні.
- Предмет дослідження: процеси поширення мовного сигналу та методи їх нейтралізації.
- Мета роботи: розробити комплекс рішень для захисту мовної інформації з урахуванням акустичних властивостей приміщення.

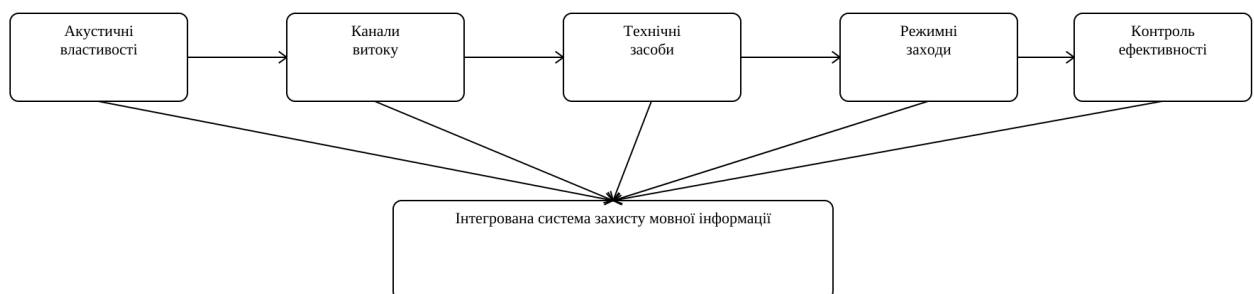
2/14

Наукові завдання та методи

- Проаналізувати методи та засоби захисту мовної інформації у контрольованих приміщеннях.
- Дослідити вплив геометрії, матеріалів, реверберації та інженерних каналів на витік сигналу.
- Розробити фізико-математичну модель поширення маскованого мовного сигналу.
- Сформувати методику оцінювання ефективності активних і пасивних заходів захисту.
- Методи: аналіз джерел, порівняльний аналіз, ризик-аналіз, акустичне моделювання, кейс-стаді.

3/14

Структура системи захисту мовної інформації



Комплексна система формується не окремими пристроями, а узгодженням акустичного аналізу, технічного захисту, режимних правил та періодичного контролю.

Акустичні властивості контрольованого приміщення

- Форма, обсяг і розміри приміщення визначають розподіл акустичної енергії.
- Паралельні стіни можуть формувати стоячі хвилі та зони підвищеної акустичної активності.
- Матеріали поверхонь впливають на відбиття, поглинання та тривалість реверберації.
- Оптимальний час реверберації для переговорних приміщень орієнтовно становить 0,4-0,6 с.

5/14

Канали витоку мовної інформації

Акустичний

Передача звуку повітрям через прорізи, двері, вікна, вентиляцію.

Віброакустичний

Поширення коливань через стіни, покриття, труби та інші конструкції.

Електроакустичний

Перетворення звуку у електричний сигнал у пристроях і комунікаціях.

Організаційний

Людський фактор, порушення правил доступу, неконтрольовані пристрої.

Виявлення каналів витоку визначає послідовність заходів: вимірювання, локалізація слабких місць, вибір технічних засобів і контроль залишкового ризику.

6/14

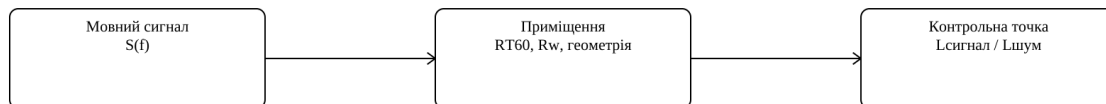
Технічні засоби захисту

- Пасивні засоби: звукопоглинальні панелі, багатошарові перегородки, ущільнені двері, акустичні екрани.
- Активні засоби: генератори шуму, системи маскування мовного сигналу, віброакустичні установки.
- Захист інженерних каналів: акустичні лабіринти, шумоглушники, демпфувальні вставки.
- Контроль технічних засобів розвідки: виявлення прихованих мікрофонів, радіопередавачів та інших пристроїв.

Організаційні та режимні заходи

- Регламентація доступу до контрольованого приміщення та ведення журналів перебування персоналу.
- Обмеження використання мобільних пристроїв та електронних носіїв у зоні конфіденційних переговорів.
- Періодичний аудит приміщення, перевірка технічних засобів і контроль стану акустичного захисту.
- Навчання персоналу правилам безпечної поведінки та реагування на можливі інциденти.

Модель поширення мовного сигналу



Модель враховує частотний спектр мовлення, звукопоглинання матеріалів, зовнішню звукоізоляцію, реверберацію та рівень маскувального шуму.

Ціль моделювання - підібрати параметри активного та пасивного захисту так, щоб за межами контрольованої зони мовлення ставало нерозбірливим.

Оцінка загроз для приміщення

- Виявляються критичні ділянки: двері, вікна, вентиляція, технологічні отвори, суміжні приміщення.
- Оцінюється інтенсивність мовного сигналу у контрольованій зоні та за її межами.
- Порівнюються рівні сигналу і маскувального шуму у частотному діапазоні мовлення.
- Формується карта ризиків для вибору пріоритетних заходів захисту.

Вибір комплексу захисту

Пасивний рівень

Звукоізоляція, звукопоглинання, ущільнення прорізів, акустичні екрани.

Активний рівень

Генератори шуму, віброакустичне маскування, адаптація спектру шуму.

Контрольний рівень

Аудит, вимірювання, перевірка каналів, оновлення акустичного паспорта.

Комплекс захисту має бути адаптований до конкретного приміщення, оскільки однакові технічні засоби дають різний ефект за різних акустичних умов.

Критерії ефективності захисту

- Зниження розбірливості мовлення за межами контрольованого приміщення.
- Досягнення необхідного запасу акустичного маскування у критичних точках контролю.
- Стабільність параметрів захисту при зміні конфігурації приміщення та присутності людей.
- Економічна доцільність: мінімізація витрат без зниження гарантованого рівня конфіденційності.

Практичні рекомендації

- Провести акустичне паспортування приміщення до введення його в експлуатацію як контрольованої зони.
- Ущільнити дверні та віконні прорізи, посилити конструктивні елементи з низькою звукоізоляцією.
- Оснастити вентиляційні канали шумоглушниками та акустичними вставками.
- Інтегрувати активне маскування з урахуванням реального спектру мовного сигналу та реверберації.
- Регулярно перевіряти ефективність захисту після ремонтів, перестановки меблів або зміни обладнання.

Загальні висновки

- Акустичні властивості приміщення безпосередньо визначають ризик витоку мовної інформації.
- Найбільш уразливими є конструктивні стики, дверні та віконні блоки, вентиляційні й інженерні канали.
- Найвищий ефект забезпечує поєднання пасивних, активних та організаційних заходів.
- Запропонований підхід дозволяє підвищити рівень конфіденційності переговорів і сформувати адаптивну систему захисту.