Київський столичний університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

«Допущено до захисту»
Завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття другого (магістерського)

рівня вищої освіти

Спеціальність 125 Кібербезпека та захист інформації

Тема роботи:

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Виконав
студент групи БІКСм-1-24-1.4.д
Романюк Валентин Сергійович

_____
(підпис)

Науковий керівник
Кандидат технічних наук, доцент
Платоненко Артем Вадимович

_____
(підпис)

Київ – 2025

Київський столичний університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

Освітньо-кваліфікаційних рівень – магістр

Спеціальність 125 Кібербезпека та захист інформації

Освітня програма 125.00.01 Безпека інформаційних і комунікаційних систем

«Затверджую»
Завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Романюку Валентину Сергійовичу

1. Тема роботи: «Дослідження шляхів та вироблення рекомендацій щодо технічного захисту інформації на об’єкті інформаційної діяльності»;
   керівник Платоненко Артем Вадимович, к.т.н., доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка,
   затверджені наказом ректора від «___»_____ 20___ року №__.
2. Термін подання студентом роботи «01» грудня 2025 р.
3. Вихідні дані до роботи:
   3.1 науково-технічна та нормативна література з теми дослідження: ідентифікація та технічний захист каналів витоку інформації на об’єкті інформаційної діяльності;
   3.2 методи: системного аналізу, фізичного та математичного моделювання каналів витоку інформації, інструментального контролю захищеності об’єктів інформаційної діяльності, оцінювання ефективності систем захисту;
   3.3 технології: активного та пасивного захисту інформації від витоку технічними каналами;
   3.4 алгоритми: оцінка захищеності акустичної інформації відповідно до чинних методик ТЗІ, ідентифікація технічних каналів витоку інформації;
   3.5 математичні моделі та методи: поширення акустичних та електромагнітних хвиль у різних фізичних середовищах.

4. Зміст текстової частини роботи (перелік питань, які потрібно розробити):
   4.1 Теоретико-методологічні засади технічного захисту інформації.
   4.2 Дослідження технічних каналів витоку на об’єкті інформаційної діяльності.
   4.3 Рекомендації щодо вдосконалення системи технічного захисту інформації.
5. Перелік графічного матеріалу:
   5.1 Презентація доповіді, виконана в Microsoft PowerPoint.
   5.2 Типові схеми: структури технічного каналу витоку; витоку інформації з контрольованої зони; генерального плану приміщення; графіків фізичних величин; система захищеного приміщення.
6. Дата видачі завдання «14» листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1.	Уточнення постановки завдання	14.11.2024	
2.	Аналіз літератури	20.12.2024	
3.	Обґрунтування вибору рішення	15.01.2025	
4.	Збір даних	25.02.2025	
5.	Виконання та оформлення розділу 1.	20.05.2025	
6.	Виконання та оформлення розділу 2.	01.09.2025	
7.	Виконання та оформлення розділу 3.	13.10.2025	
8.	Вступ, висновки, реферат	20.10.2025	
9.	Апробація роботи на науковометодичному семінарі та/або науково-технічній конференції	26.10.2025	
10.	Оформлення та друк текстової частини роботи	10.11.2025	
11.	Оформлення презентацій	12.11.2025	
12.	Отримання рецензій	14.11.2025	
13.	Попередній захист роботи	21.11.2025	
14.	Захист в ЕК	17.12.2025	

Студент _____ Романюк Валентин Сергійович
(підпис) (прізвище, ім’я, по батькові)

Науковий керівник _____ Платоненко Артем Вадимович
(підпис) (прізвище, ім’я, по батькові)

РЕФЕРАТ

Кваліфікаційна робота присвячена технологіям використання комплексних систем технічного захисту інформації в системах обробки конфіденційної інформації на об’єктах інформаційної діяльності.

Робота складається зі вступу, трьох розділів, що містять 15 рисунків та 9 таблиць, висновків та списку використаних джерел, що містить 15 найменувань. Загальний обсяг роботи становить 74 сторінки, з яких сторінки займають ілюстрації і таблиці на окремих аркушах, а також додатки, перелік умовних скорочень та список використаних джерел.

Об’єктом дослідження в роботі є процес витоку інформації з обмеженим доступом технічними каналами на об’єктах інформаційної діяльності.

Предметом дослідження є метод методи та засоби технічного захисту мовної та видової інформації від витоку акустичними, віброакустичними та електромагнітними каналами.

Метою роботи є підвищення рівня захищеності мовної та візуальної інформації на об’єкті інформаційної діяльності шляхом розробки та обгрунтування комплексу організаційно-технічних заходів протидії витоку інформації технічними каналами.

Для досягнення поставленої мети у роботі:

проведено аналіз існуючих підходів до класифікації загроз та нормативно правового регулювання у сфері технічного захисту інформації;

досліджено особливості фізичних принципів формування технічних каналів витоку, зокрема віброакустичних та електромагнітних, на прикладі виділеного приміщення;

обґрунтовано доцільність застосування систем активного віброакустичного зашумлення та пасивного екранування інтерфейсних кабелів для нейтралізації виявлених загроз.

Наукова новизна одержаних результатів полягає в тому, що в роботі удосконалено методику комплексної оцінки захищеності виділеного приміщення шляхом поєднання інструментального контролю віброакустичних каналів з

аналізом спектральних характеристик побічних випромінювань сучасних відеоінтерфейсів, та дістало подальший розвиток обґрунтування застосування комбінованих методів захисту вентиляційних каналів.

Галузь застосування. Запропоновані підходи можуть бути використані для створення або модернізації комплексних систем захисту інформації на підприємствах та в державних установах, що здійснюють обробку інформації з обмеженим доступом.

Ключові слова: БЕЗПЕКА, ЗАГРОЗА, ІНФОРМАЦІЯ, ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, КАНАЛ ВИТОКУ, ВІБРОАКУСТИЧНИЙ ЗАХИСТ, ПЕМВН, СИСТЕМА ЗАХИСТУ.

ЗМІСТ

Ст.

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ДТЗС – допоміжні технічні засоби

ДСТУ – державний снадарт України

ЗТР – засіб технічної розвідки

ІзОД – інформація з обмеженим доступом

КЗ – контрольована зона

КСТЗІ – комплексна система технічного захисту інформації

НД – нормативний документ

НСД – несанкціонований доступ

ОІД – об’єкт інформаційної діяльності

ОТЗ – основні технічні засоби

ПЕМВН – побічні електромагнітні випромінювання і наводки

САЗ – система активного акустичного зашумлення

СТЗІ –системи технічного захисту інформації

ТЗІ – технічний захист інформації

ТКВІ – технічні канали витоку інформації

ВСТУП

Актуальність теми. В умовах гібридної війни та стрімкої глобальної цифровізації, інформація трансформувалася в критичний стратегічний ресурс. За даними Державної служби спеціального зв'язку та захисту інформації України, кількість кіберінцидентів, спрямованих на державний сектор, енергетику та об'єкти критичної інфраструктури, у 2022-2023 роках зросла майже втричі порівняно з довоєнним періодом [1]. Основною ціллю зловмисників стають не лише інформаційно-телекомунікаційні системи, а й місця прийняття управлінських рішень, де циркулює мовна інформація з обмеженим доступом.

Згідно зі світовою статистикою IBM Security Cost of a Data Breach Report, середня вартість витоку даних для підприємства у 2023 році досягла історичного максимуму, перевищивши 4,45 млн доларів США [2], причому значна частка інцидентів пов'язана з інсайдерськими загрозами та фізичним доступом до інфраструктури. Дані комерційного сектору ілюструють масштаб проблеми, який для об'єктів критичної інфраструктури та державних органів трансформується у загрози національній безпеці. Вразливість сучасних об'єктів інформаційної діяльності посилюється широким використанням новітніх мультимедійних засобів, які, не маючи належного захисту, створюють нові, часто неконтрольовані, канали витоку інформації за рахунок побічних електромагнітних випромінювань [3].

Проблема ускладнюється тим, що існуючі на більшості підприємств системи захисту побудовані за застарілими шаблонами, орієнтованими переважно на мережеву безпеку, ігноруючи фізичні та технічні канали витоку. Як наслідок, зловмисники, використовуючи сучасні засоби технічної розвідки отримують можливість безконтактного знімання інформації з-за межами контрольованої зони.

В якості системної методології вирішення цієї проблеми сучасна наука пропонує перехід від жорсткого детермінованого захисту до ризик-орієнтованого підходу, відповідно до стандартів ISO/IEC 27000. Проте практична реалізація цього підходу на об'єктах інформаційної діяльності стикається з низкою проблем:

1. відсутність адаптованих методик інструментального контролю новітніх цифрових інтерфейсів;
2. складність виявлення комбінованих каналів витоку;
3. недостатнє обгрунтування ефективності засобів активного захисту з точки зору санітарних норм та комфорту персоналу;
4. висока вартість професійного вимірювального обладнання, що унеможливлює регулярний моніторинг захищеності на малих та середніх підприємствах.

Застосування удосконалених інструментально-розрахункових методів та розробка комплексних інженерних рішень дозволяє вирішити ці протиріччя. Вищезазначене підтверджує актуальність теми магістерської роботи та її доцільність для практики у сфері технічного захисту інформації.

Мета роботи полягає у підвищені рівня захищеності каналів витоку інформації на об’єкті інформаційної діяльності шляхом розробки та обгрунтування комплексу організаційно-технічних заходів протидії витоку інформації технічними каналами.

Для досягнення поставленої мети необхідно вирішити такі **завдання**:

1. Провести аналіз теоретико-методологічних засад технічного захисту інформації, класифікувати загрози та визначити особливості нормативно-правового регулювання захисту інформації в Україні.
2. Здійснити аналіз технічних каналів витоку інформації та сучасних засобів технічної розвідки.
3. Провести комплексне обстеження виділеного приміщення, виявити потенційні канали витоку та дослідити їх захищеність.
4. Розробити обгрунтовані рекомендації щодо вдосконалення системи захисту, включаючи вибір засобів активної та пасивної протидії, та розрахувати їх ефективність.

Об’єкт дослідження - процес витоку інформації з обмеженим доступом технічними каналами на об’єкті інформаційної діяльності.

Предмет дослідження - методи та засоби технічного захисту мовної та видової інформації від витоку акустичними, віброакустичними та електромагнітними каналами.

Методи дослідження. У роботі використано комплексний підхід, що базується на поєднанні теоретичних та практичних методів. Зокрема, методи аналізу застосовано для систематизації нормативної бази та класифікації загроз. Метод моделювання використано для опису фізичних процесів утворення каналів витоку. Інструментально-розрахунковий метод дозволив визначити коефіцієнт словесної розбірливості мови та оцінити ефективність віброакустичного захисту. Спектральний аналіз застосовано для виявлення та ідентифікації побічних електромагнітних випромінювань від інтерфейсних кабелів, а експертний метод послугував основою для вибору раціонального комплексу засобів захисту.

Наукова новизна одержаних результатів. У дипломній роботі удосконалено методику комплексної оцінки захищеності виділеного приміщення шляхом поєднання інструментального контролю віброакустичних каналів з аналізом спектральних характеристик побічних випромінювань сучасних відеоінтерфейсів, зокрема стандарту HDMI та USB. Також отримало подальший розвиток рекомендацій застосування комбінованих методів захисту вентиляційних каналів, що поєднують активні та пасивні засоби, що дозволяє забезпечити акустичну непрозорість вентиляції при збереженні комфортних умов праці.

Практичне значення одержаних результатів. Розроблені рекомендації та технічні рішення можуть бути безпосередньо використані для створення або модернізації комплексних систем захисту інформації на підприємствах та в установах. Запропонована схема розміщення вібровипромінювачів та методика використання портативних аналізаторів спектра дозволяють підвищити ефективність захисту кімнат проведення конференцій, де обробляється інформація з обмеженим доступом, від сучасних засобів викрадення інформації.

Галузь застосування. Створення систем технічного захисту інформації державних установ, органів місцевого самоврядування та комерційних структур, що здійснюють обробку інформації з обмеженим доступом.

Апробація результатів дипломної роботи. Основні положення роботи викладалися:

1. в статті журналу «Кібербезпека: освіта, наука, техніка» , Том 1 № 29 (2025)[4];
2. в тезах доповіді на Студентській науковій конференції «Безпека інформаційно-комунікаційних систем» (Київ: Київський столичний університет імені Бориса Грінченка, 26 жовтня 2025 року) [5].

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

1.1. Інформація як об’єкт захисту та понятійний апарат системи ТЗІ

В умовах стрімкого розвитку інформаційного суспільства та глобальної цифровізації усіх сфер життєдіяльності, інформація трансформувалася з допоміжного ресурсу в стратегічний актив, що визначає успішність функціонування як державних інституцій, так і приватних підприємств. У сучасному світі інформація набула яскраво вираженої двобічної природи. З одного боку, вона виступає як капітал та ресурс розвитку, втрата якого призводить до прямих фінансових збитків та втрати конкурентних переваг. З іншого боку, в умовах гібридних конфліктів та корпоративних воєн, інформація стає потенційним джерелом ризиків і зброєю: її витік може призвести до компрометації системи управління, репутаційних катастроф та руйнування соціально-політичної обстановки. Така подвійна сутність зумовлює необхідність створення надійної, багаторівневої системи захисту.

Технічний захист інформації (ТЗІ) займає особливе місце в загальній архітектурі інформаційної безпеки, виступаючи її інженерно-технічним фундаментом. Якщо криптографічний захист орієнтований на математичне перетворення даних, а організаційні заходи - на контроль дій персоналу, то роль ТЗІ полягає у створенні фізичних та апаратних бар’єрів у реальному просторі. Головна мета ТЗІ - забезпечити неможливість несанкціонованого доступу до інформаційних ресурсів через фізичні канали витоку навіть за умови, що зловмисник володіє найсучаснішими засобами розвідки. Без надійного технічного захисту будь-які логічні методи захисту можуть бути усунені шляхом прямого фізичного знімання сигналів.

Для глибшого розуміння цілей захисту доцільно звернутися до міжнародної методології, закріпленої у стандартах серії ISO/IEC 27000. Згідно з нею, інформаційна безпека розглядається як забезпечення трьох фундаментальних властивостей інформації:

- Конфіденційність - властивість інформації бути недоступною або закритою для неавторизованих осіб, сутностей чи процесів. У контексті ТЗІ основна мета - це запобігання витоку через технічні канали.
- Цілісність - властивість захисту точності та повноти активів. ТЗІ забезпечує це шляхом унеможливлення несанкціонованої модифікації сигналів або введення хибних даних.
- Доступність - властивість бути доступним і придатним до використання на вимогу авторизованої сутності. Хоча ТЗІ менше фокусується на цьому аспекті, захист від блокування сигналів або фізичного руйнування носіїв також є частиною комплексної безпеки.

Для однозначного тлумачення предметної області дослідження та уникнення термінологічних колізій необхідно визначити базовий понятійний апарат. Він спирається на чинну нормативно-правову базу України, зокрема Закони України «Про захист інформації в інформаційно-комунікаційних системах» [6], «Про державну таємницю» [7] та базові стандарти (ДСТУ 3396.2-97).

Ключовим поняттям даного дослідження є об’єкт інформаційної діяльності (ОІД). Згідно з українським законодавством, ОІД визначається не просто як абстрактна інформаційна система чи набір даних, а як конкретне фізичне середовище. Це інженерно-технічна споруда, виділене приміщення, транспортний засіб або територіальна зона, де здійснюється діяльність, пов’язана з інформацією, що підлягає захисту. Саме просторова класифікація ОІД визначає специфіку технічного захисту: на відміну від кібербезпеки, де захищається логічний периметр мережі, в ТЗІ необхідно захищати фізичний периметр - будівельні конструкції, вікна, двері та інженерні комунікації, що виходять за межі об’єкта.

Невід'ємною складовою ОІД є контрольована зона (КЗ) - це територія навколо об’єкта, на якій організаційними заходами виключено неконтрольоване перебування сторонніх осіб, що не мають права доступу, а також унеможливлене несанкціоноване розміщення технічних засобів розвідки (транспорту, стороннього обладнання, приймальних антен). Межа контрольованої зони є критично важливою точкою відліку для проєктування системи захисту, оскільки саме на ній

відбувається перехоплення фізичних полів, енергія яких затухає з відстанню. Завдання системи захисту - гарантувати, що рівень інформативного сигналу на межі КЗ буде нижчим за поріг чутливості засобів розвідки.

Безпосередньо ТЗІ визначається як - специфічний вид захисту, спрямований на забезпечення за допомогою інженерно-технічних заходів, програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації. Слід особливо підкреслити, що українська нормативна база ставить перед ТЗІ жорстку вимогу унеможливлення, на відміну від поширеного у міжнародних стандартах ризик-орієнтованого підходу мінімізації ризиків. Це вимагає від розробника комплексної системи захисту інформації застосування гарантованих методів блокування каналів витоку, а не лише ймовірнісних заходів.

Фундаментальним поняттям для побудови моделі загроз є технічний канал витоку інформації (ТКВІ). Під цим терміном розуміють сукупність трьох обов’язкових елементів:

- джерело інформативного сигналу - фізичний процес, параметри якого змінюються відповідно до змісту інформації;
- фізичне середовище поширення - матеріальне середовище, через яке сигнал передається від джерела за межі контрольованої зони;
- технічний засіб розвідки - апаратура зловмисника, здатна перехопити сигнал, підсилити його та виділити інформативні ознаки на фоні завад.

Розуміння фізичної природи утворення ТКВІ є основою для розробки вірної моделі загроз. Ефективна протидія можлива лише шляхом впливу на один з елементів цієї тріади: локалізація джерела, зміна властивостей середовища або створення активних завад для приймача.

1.2. Нормативно-правове регулювання захисту інформації в Україні

Побудова ефективної системи ТЗІ неможлива без глибокого розуміння та чіткого дотримання вимог чинного законодавства. В Україні на сьогодні сформована розгалужена та ієрархічна система нормативно-правового регулювання, яка охоплює всі аспекти інформаційної безпеки - від загальних конституційних гарантій до специфічних інженерних методик вимірювання

сигналів. Ця система має яскраво виражену структуру, що складається з кількох рівнів юридичної сили.

Фундаментальний рівень формує Конституція України та Кодекси, які закріплюють інформаційний суверенітет держави та права власників на захист своєї інформації. Наступним, стратегічним рівнем, є Закони України. Вони визначають державну політику, встановлюють правові режими доступу до інформації (відкрита, таємна, службова) та покладають відповідальність за її збереження. Саме закони встановлюють вимогу створення систем захисту інформації для державних інформаційних ресурсів.

Реалізація законодавчих норм на практиці забезпечується через систему підзаконних актів - Указів Президента та Постанов Кабінету Міністрів. Ці документи регламентують конкретні процедури: як саме створювати системи захисту, як проводити їх експертизу та хто здійснює контроль. Головним регулятором у цій сфері виступає Державна служба спеціального зв'язку та захисту інформації України, яка формує нормативно-технічну політику галузі.

Для інженерно-технічного персоналу найбільш важливим є рівень нормативних документів технічного захисту інформації (НД ТЗІ) та державних стандартів (ДСТУ). Це суто технічні документи, що містять конкретні методики, формули розрахунків, вимоги до обладнання та критерії оцінки захищеності. Без дотримання вимог НД ТЗІ неможливо отримати Атестат відповідності на об'єкт інформаційної діяльності.

Україна також активно використовує міжнародні стандарти серії ISO/IEC 27000. Вони формують альтернативний контур регулювання, який базується на ризико-орієнтованому підході. Якщо національні НД ТЗІ дають чітку інструкцію «як зробити», то стандарти ISO відповідають на питання «як управляти процесом», що є критично важливим для сумісності з міжнародними партнерами.

Систематизований перелік ключових нормативно-правових актів, що регулюють сферу ТЗІ та використовуються у даному магістерському дослідженні, наведено в таблиці 1.1.

Таблиця 1.1

Нормативно-правова база технічного захисту інформації

Рівень регулювання	**Назва документа**	**Сфера регулювання та значення для дослідження**
Законодавчий	ЗУ «Про інформацію» [8]	Визначає основні види інформації, правові режими доступу та гарантії захисту
	ЗУ «Про захист інформації в інформаційно-комунікаційних системах»	Базовий закон галузі. Встановлює обов'язковість захисту інформації, що є власністю держави, та вводить поняття КСЗІ
	ЗУ «Про державну таємницю»	Регламентує процедури віднесення інформації до державної таємниці та вимоги до режиму секретності на об'єктах
	ЗУ «Про основні засади забезпечення кібербезпеки України»	Визначає засади захисту життєво важливих інтересів у кіберпросторі та захист критичної інфраструктури
Підзаконний	Постанова КМУ № 373 від 29.03.2006	Затверджує «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»
Нормативно-технічний	НД ТЗІ 1.6-005-2013	«Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання». Визначає процедуру присвоєння категорії ОІД
	НД ТЗІ 2.5-004-99	«Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Встановлює класи захищеності (АС-1, АС-2 тощо)

Продовження табл. 1.1

	НД ТЗІ 2.3-017-08	«Методика контролю захищеності мовної інформації від витоку акустичним та віброакустичним каналами»
Міжнародні стандарти	ДСТУ ISO/IEC 27001:2023	Визначає вимоги до системи управління інформаційною безпекою (СУІБ). Базується на управлінні ризиками
	ДСТУ ISO/IEC 27005	Стандарт з менеджменту ризиків інформаційної безпеки. Описує процес ідентифікації та обробки загроз

Аналіз нормативної бази дозволяє зробити висновок про існування двобічної моделі регулювання. Для захисту державних ресурсів застосовується метод суворої регламентації, тоді як для комерційного сектору - метод саморегулювання. Дане дослідження базується на об’єднані цих підходів: використання інженерної точності методик НД ТЗІ для блокування технічних каналів витоку та принципів системності, закладених у міжнародних стандартах.

1.3. Технічні канали витоку. Загальні поняття

У сучасній теорії та практиці захисту інформації на ОІД центральне місце займає проблематика запобігання несанкціонованому доступу до конфіденційних даних. Фундаментальним поняттям у цьому контексті виступає витік інформації, який визначається як процес неконтрольованого поширення даних, що захищаються, за межі встановленого власником кола осіб або території, що у підсумку призводить до їх отримання сторонніми особами. Оскільки реалізація такого перехоплення з боку зловмисника, як правило, здійснюється із застосуванням спеціального технічного обладнання, самі шляхи переміщення інформації отримали назву технічних каналів. У загальному вигляді технічний канал витоку інформації являє собою сукупність фізичного шляху, яким інформаційний сигнал переміщується у просторі від джерела його виникнення до приймального пристрою технічної розвідки[9].

Структурна будова будь-якого технічного каналу витоку є складною системою взаємопов’язаних елементів. Для існування реальної загрози необхідна одночасна наявність трьох компонентів: джерела небезпечного сигналу, фізичного середовища, в якому цей сигнал може поширюватися, та власне засобу технічної розвідки (ЗТР), здатного цей сигнал зареєструвати та дешифрувати (рис.1.1).

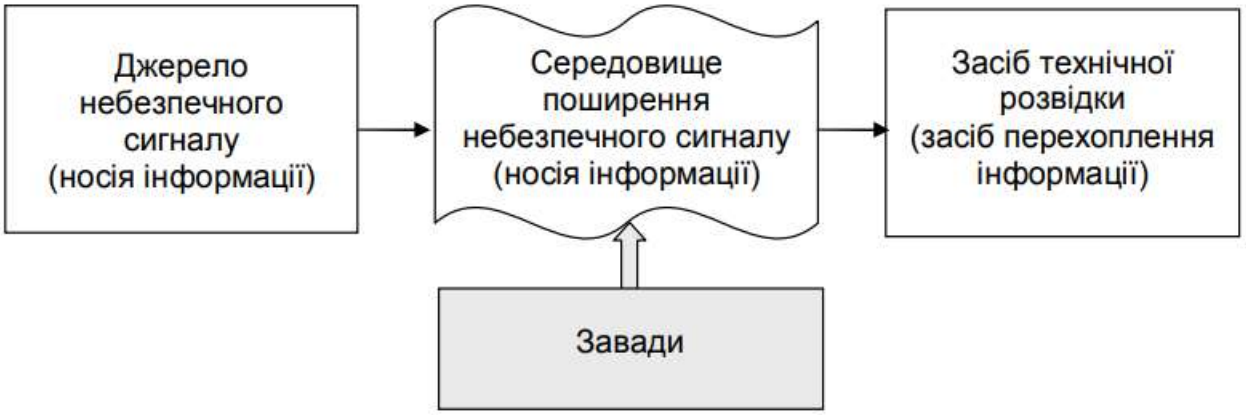

Рис. 1.1 Технічний канал витоку інформації

При аналізі ефективності такого каналу також обов’язково необхідно враховувати наявність та рівень завад, що діють на вході розвідувального приймача, оскільки природні або штучні шуми можуть суттєво ускладнити або унеможливити відновлення корисної інформації зловмисником.

Першопричиною утворення каналу витоку є наявність небезпечного сигналу. Під цим терміном розуміють будь-які сигнали або фізичні поля, зокрема й ті, що мають паразитний чи побічний характер, які містять у своїй структурі відомості з обмеженим доступом. Цей сигнал нерозривно пов’язаний із поняттям носія інформації - фізичного явища або матеріального об’єкта, що безпосередньо здійснює перенесення даних. Спектр можливих носіїв є досить широким і охоплює різноманітні фізичні стани: від електричного струму та електромагнітних полів різного діапазону, включно зі світловим та лазерним випромінюванням, до акустичних коливань і вібраційних полів, що виникають у твердих тілах. Крім того, носіями можуть виступати матеріальні об’єкти, такі як хімічні речовини чи інші матеріали.

Критично важливу роль у формуванні каналу відіграє середовище поширення сигналу. Інформативні носії можуть розповсюджуватися через повітряний простір, воду, ґрунт або будівельні конструкції. Найбільшу загрозу з точки зору технічного захисту становлять струмопровідні комунікації та металеві конструкції, які виходять за межі контрольованої зони об’єкта. До таких елементів відносяться лінії електроживлення, контури заземлення, телефонні кабелі, системи сигналізації, труби опалення та водопостачання, а також арматура залізобетонних конструкцій. Засоби технічної розвідки можуть перехоплювати сигнал як дистанційно у вільному просторі, так і шляхом безпосереднього підключення до зазначених комунікацій за межами об’єкта.

На об’єктах інформаційної діяльності джерелами небезпечних сигналів стають процеси обробки та обігу інформації. Це може бути озвучування відомостей людьми або звукопідсилювальною апаратурою, обробка даних в електронних системах, а також візуалізація інформації на екранах моніторів чи у вигляді роздрукованих документів. З метою ефективної організації захисту все технічне обладнання на об’єкті підлягає чіткій класифікації. Технічні засоби, які безпосередньо беруть участь в обробці, зберіганні або передачі секретної інформації, відносять до категорії основних технічних засобів і систем. Саме вони є генераторами небезпечних сигналів, що поширюються у навколишній простір.

Окрему групу обладнання становлять допоміжні технічні засоби та системи (ДТЗС). До них належать пристрої, що не призначені для обробки таємних даних, проте необхідні для функціонування об’єкта: системи міського телефонного зв’язку, пожежної та охоронної сигналізації, побутова техніка тощо. Небезпека полягає в тому, що ДТЗС, знаходячись поруч із основними засобами, потрапляють під вплив їхніх електромагнітних полів. У результаті цього явища в ланцюгах допоміжних засобів або у сторонніх провідниках можуть наводитися інформативні сигнали, перетворюючи їх на випадкові антени, через які інформація може транслюватися за межі об’єкта. Схематично можливість витоку інформації наведена на рис.1.2.

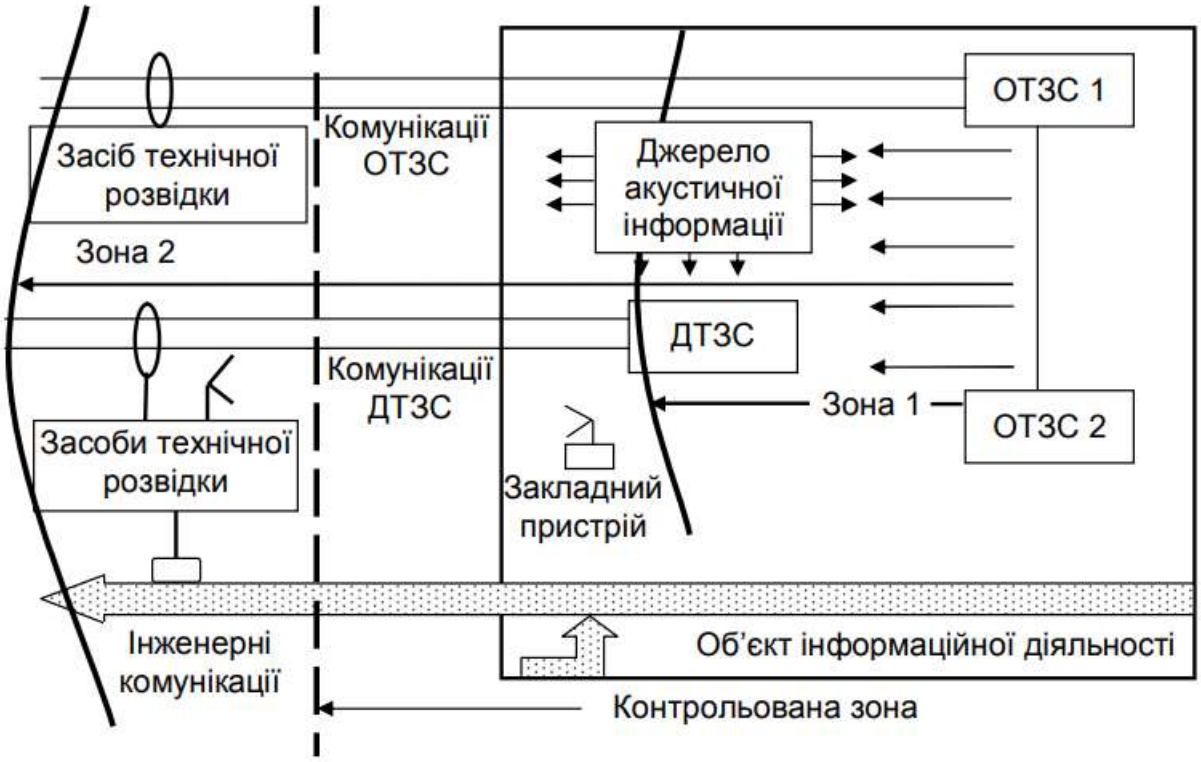

Рис. 1.2 Схематична можливість витоку інформації

Фізичні властивості електромагнітних, акустичних, вібраційних полів такі, що їх енергія неминуче згасає зі збільшенням відстані від джерела. Це дозволяє визначити просторові межі, за якими перехоплення інформації стає технічно неможливим через падіння рівня сигналу нижче рівня шумів. На основі цього принципу базуються пасивні методи захисту та зонування території навколо основних технічних засобів. Для кожного комплекту обладнання експериментально-розрахунковим шляхом визначаються дві ключові зони безпеки: Зона 1 та Зона 2.

Зона 2 характеризує простір, де можливе пряме перехоплення інформативного сигналу засобами розвідки. Вона окреслюється радіусом R2, за межами якого співвідношення сигнал/шум стає недостатнім для відновлення інформації. Для унеможливлення витоку навколо об'єкта повинна бути створена та організаційно забезпечена контрольована зона. Межа цієї контрольованої зони повинна знаходитись на відстані, що перевищує радіус Зони 2.

Зона 1, радіус якої R1, зазвичай менший за радіус Зони 2, визначає простір навколо ОТЗ, де напруженість електромагнітного поля є достатньою для наведення

небезпечних сигналів у сторонніх провідниках та лініях допоміжних систем. Якщо такі провідники або кабелі ДТЗС проходять через Зону 1 і далі виходять за межі контрольованої зони, виникає загроза витоку інформації через наведення. Хоча випадкові антени є менш ефективними, ніж спеціальні, наближення засобів розвідки до таких комунікацій може дозволити зняти інформацію. Тому однією з головних вимог технічного захисту є розміщення допоміжних засобів та сторонніх провідників поза межами Зони 1.

1.4. Класифікація технічних каналів витоку інформації

Фундаментальною основою технічного захисту інформації є розуміння того факту, що будь-який процес обробки, передачі або зберігання інформації нерозривно пов’язаний зі зміною фізичних параметрів носія. Сутність процесу витоку полягає в тому, що частина енергії інформаційного сигналу, чи то акустичного, чи електромагнітного, неминуче розсіюється в навколишній простір або наводиться на сторонні провідники. Якщо енергія цього розсіяного сигналу перевищує поріг чутливості засобів розвідки на межі контрольованої зони, канал витоку вважається реалізованим.

Систематизація технічних каналів витоку здійснюється за двома ключовими критеріями: фізичною природою носія та середовищем його поширення.

Серед усього спектру загроз інформаційній безпеці акустичні та віброакустичні канали займають особливе місце, оскільки вони пов'язані з безпосереднім перехопленням первинного носія мовної інформації - звукової хвилі. Фізичною основою утворення цих каналів є здатність звуку поширюватися у будь-якому пружному середовищі, будь то гази, рідини чи тверді тіла. Залежно від середовища поширення та механізму перехоплення, ці канали поділяються на дві великі групи, кожна з яких має свої специфічні фізичні особливості та методи захисту.

Першою групою є акустичні канали, де середовищем поширення виступає повітря. Витік інформації відбувається за рахунок того, що звукова хвиля, яка генерується голосовим апаратом людини, поширюється від джерела заповнюючи весь об'єм приміщення. Критичними вразливостями у цьому випадку є будь-які

наскрізні отвори та нещільності в огороджувальних конструкціях. Найбільшу небезпеку становлять системи вентиляції та кондиціонування, які фактично є порожнистими хвилеводами. Металеві стінки вентиляційних коробів мають високий коефіцієнт відбиття звуку, що дозволяє акустичному сигналу поширюватися на значні відстані з мінімальним загасанням, виходячи за межі контрольованої зони на дах або фасад будівлі. Крім того, слабкими місцями є дверні отвори та технологічні отвори для розеток у суміжних стінах. Для перехоплення інформації в акустичному каналі зловмисник може використовувати високочутливі мікрофони, розміщені у вентиляційних шахтах, або спрямовані мікрофони параболічного типу для дистанційного запису через відкриті кватирки.

Другою, більш складною для виявлення групою, є віброакустичні канали. Вони виникають внаслідок переходу енергії повітряної звукової хвилі в енергію механічних коливань твердого тіла. Коли звукова хвиля переходить на перешкоду, виникає змінний тиск, який змушує цю перешкоду вібрувати з частотою мовного сигналу. Інтенсивність цих вібрацій залежить від маси та пружності матеріалу: легкі конструкції, такі як віконне скло або гіпсокартонні перегородки, мають значну амплітуду коливань і є чудовими ретрансляторами звуку. Масивні конструкції, наприклад стіни, вібрують значно слабше, але завдяки високій густині матеріалу та малим внутрішнім втратам, здатні передавати ці мікроколивання на великі відстані в межах будівлі.

Особливу роль у формуванні віброакустичних каналів відіграють інженерні комунікації, зокрема труби систем опалення, водопостачання та газопроводу. Металеві труби та рідина, що їх заповнює, є ідеальними провідниками звуку, швидкість поширення якого у воді та сталі в кілька разів перевищує швидкість ніж у повітрі. Це дозволяє зловмиснику перехоплювати розмови з приміщень, розташованих на декілька поверхів вище або нижче, просто приставивши датчик до труби-стояка. Для знімання інформації з твердих поверхонь використовуються контактні мікрофони - електронні стетоскопи, які перетворюють механічні вібрації стіни чи труби назад в електричний сигнал. Такий спосіб перехоплення є надзвичайно небезпечним, оскільки датчик може бути встановлений у сусідньому

приміщенні або на зовнішній стіні будівлі, тобто поза межами візуального контролю служби безпеки об’єкта.

Третю групу становлять електромагнітні канали, або радіоканали, пов’язані з поширенням електромагнітних хвиль у просторі. Електромагнітний канал витоку інформації, який базується на перехопленні побічних електромагнітних випромінювань та наводок (ПЕМВН), є одним із найбільш небезпечних та інформативних каналів у системі технічного захисту. Його фізична природа обумовлена фундаментальними законами електродинаміки, згідно з якими будь-який провідник зі змінним електричним струм є джерелом електромагнітного поля. У контексті сучасних об’єктів інформаційної діяльності найбільшу загрозу становлять випромінювання від високошвидкісних цифрових інтерфейсів передачі відеоданих, які замінили застарілі аналогові стандарти.

Особливістю сучасних відеоінтерфейсів є використання технології диференціальної передачі сигналів. Передача даних здійснюється пакетами цифрових імпульсів з дуже високою тактовою частотою. Механізм формування каналу витоку реалізується за умови, коли інтерфейсний кабель пристрою діє як випадкова антена. Аналіз фізичних процесів виникнення каналів витоку інформації, наведений у фундаментальних працях В.О. Хорошка та А.А. Чекаткова [10], свідчить про критичну роль випадкових антен у формуванні побічних електромагнітних випромінювань. Зокрема, ефективність випромінювання різко зростає при порушенні цілісності екранування, використання неякісних кабелів або виникнення резонансних явищ, коли довжина кабелю стає кратною половині або чверті довжини хвилі випромінюваного сигналу. Такі паразитні антени формують навколо об’єкта електромагнітне поле, що містить інформативні ознаки оброблюваної інформації, що створює передумови для її несанкціонованого перехоплення.

Залежно від потужності джерела та умов поширення, навколо технічного засобу формуються дві небезпечні зони. Зона 1 - це простір, у межах якого можливе перехоплення інформації засобами радіорозвідки з високою ймовірністю. Зона 2 - це зона, де можливе виділення інформативного сигналу на фоні шумів за

допомогою спеціальних методів обробки. Сучасні засоби технічної розвідки, такі як портативні аналізатори спектра та програмно-визначені радіосистеми, здатні виявляти частоти відеосигналу на відстані десятків метрів, що часто виходить за межі контрольованої зони приміщення. Оскільки амплітуда цих коливань залежна зі зміною яскравості пікселів на екрані, зловмисник має технічну можливість здійснити зворотне перетворення перехопленого радіосигналу у відеозображення, повністю відновивши інформацію, що відображається на моніторі користувача.

Четверта група - це електричні або провідні канали. Фізичним носієм інформації в таких каналах виступає електричний струм або напруга. Це може бути як корисний сигнал, що передається лініями зв’язку, так і паразитний сигнал наведення, що виникає випадково. Специфіка цієї групи загроз полягає у тому, що металеві комунікації часто мають велику протяжність і виходять далеко за межі контрольованої зони об'єкта, створюючи для зловмисника зручну можливість підключення без необхідності фізичного проникнення у приміщення.

Основним середовищем поширення небезпечних сигналів у цій групі є будь-які струмопровідні комунікації та конструкції. Їх перелік значно ширший, ніж просто електричні дроти. До цього середовища належать штатні лінії електромережі, системи заземлення, телефонні кабелі, лінії пожежної та охоронної сигналізації, а також комп’ютерні мережі. Окрім спеціально прокладених кабелів, роль провідника можуть виконувати так звані сторонні провідники - металеві елементи інфраструктури будівлі, які не призначені для передачі інформації, але мають властивість електропровідності. Сюди відносяться труби систем опалення, водопостачання та газопроводу, металева арматура залізобетонних стін, вентиляційні короби та екрануючі обплетення кабелів. Всі ці елементи утворюють розгалужену мережу, якою високочастотний сигнал може поширюватися на значні відстані з мінімальним затуханням.

Джерелом небезпеки утворення каналу витоку є підключення технічних засобів обробки інформації та засобів сторонніх споживачів до спільного джерела живлення або контуру заземлення. Через недосконаліть технічних рішень або відсутність розв’язуючих пристроїв, інформативні сигнали можуть просочуватися

в мережу електроживлення. Внаслідок цього в розетках сусідніх приміщень або навіть сусідніх будівель, що живляться від тієї ж трансформаторної підстанції, з’являється високочастотна складова, яка містить захищувані дані. Для реалізації перехоплення зловмиснику достатньо легально підключити спеціальний аналізатор мережі до звичайної розетки поза межами приміщення.

Окрему загрозу в рамках цієї групи становить безпосереднє контактне підключення до ліній зв’язку та передачі даних. Це може бути реалізовано шляхом несанкціонованої врізки в кабель або встановлення спеціальних апаратних закладок у комутаційних шафах, розетках чи розподільчих коробках. Такі пристрої можуть перехоплювати інформацію та передавати її далі по тій же лінії на іншій частоті, яка не використовується штатним обладнанням, або ж накопичувати дані для подальшого зчитування. Складність виявлення таких каналів полягає у тому, що підключення може бути здійснене у важкодоступних місцях інженерних комунікацій, а пасивні методи знімання інформації практично не вносять завад у роботу основної лінії.

П’ята група класифікації охоплює широкий спектр оптичних каналів витоку, функціонування яких грунтується на фізичних закономірностях поширення електромагнітних хвиль оптичного діапазону. На відміну від радіочастотних каналів, де носієм виступає радіохвиля, тут передача даних відбувається за допомогою фотонних потоків. Фізичним носієм інформації в таких системах є світловий промінь, який може належати до різних ділянок спектра: видимого світла, що сприймається людським оком, а також невидимих для людини інфрачервоного та ультрафіолетового діапазонів. Середовищем поширення сигналу в оптичних каналах найчастіше виступає повітряний простір, проте передача може також відбуватися через оптично прозорі матеріали, такі як віконне скло, лінзи приладів або спеціалізовані волоконно-оптичні кабелі. Специфічною рисою цієї групи є, як правило, необхідність наявності прямої видимості між джерелом сигналу та приймачем зловмисника, що робить світлопрозорі огороджувальні конструкції найбільш вразливими елементами в системі захисту приміщення.

Основним та найбільш поширеним різновидом загроз у цій групі є візуально-оптичне спостереження. Цей метод базується на отриманні видової інформації шляхом реєстрації відбитого світла від об’єктів спостереження або ж власного випромінювання джерел світла. Спостереження може вестися як неозброєним оком, так і з використанням складних оптичних та оптико-електронних приладів: біноклів, телескопів, приладів нічного бачення та тепловізорів. Застосування довгофокусної оптики дозволяє зловмисникам багаторазово наближати зображення, що створює реальні можливості для дистанційного читання текстових документів, залишених на робочих столах, а також зчитування інформації безпосередньо з екранів комп’ютерних моніторів та дисплеїв іншого офісного обладнання. Окрім статичної інформації, оптичний канал дозволяє отримувати динамічні дані, зокрема, проводити відновлення змісту розмов шляхом розпізнавання артикуляції губ співрозмовників. Сучасні цифрові камери, оснащені матрицями високої роздільної здатності та системами оптичної стабілізації зображення, здатні фіксувати чітку картинку навіть в умовах недостатнього освітлення, через частково зашторені вікна або з рухомих транспортних засобів, що значно ускладнює виявлення факту шпигунства.

Окремою категорією є параметричні канали витоку, які виникають при зміні параметрів середовища або елементів схем під впливом інформаційного сигналу. Класичним прикладом є створення високочастотного сигналу, що опромінює приміщення, акустичними коливаннями, які змінюють ємність або індуктивність елементів, що відоме як ефект ВЧ-нав’язування.

Слід зазначити, що в реальних умовах канали часто комбінуються[11]. Наприклад, акустична хвиля, створена голосом, збуджує вібрацію віконного скла, яка потім зчитується лазерним променем через оптичний канал. Таке явище називається трансформацією каналів витоку і є найбільш складним для виявлення та блокування.

1.5. Сучасні засоби технічної розвідки та їх можливості

Аналіз фізичних принципів формування каналів витоку інформації дозволяє систематизувати арсенал сучасних засобів технічної розвідки, що можуть бути

застосовані зловмисниками для перехоплення інформації. Ефективність реалізації загрози прямо залежить від технічних характеристик приймальної апаратури, її чутливості та можливості прихованого застосування. Залежно від фізичної природи перехоплюваного сигналу, засоби розвідки поділяються на кілька функціональних груп.

Для практичної експлуатації акустичних та віброакустичних каналів витоку зловмисниками застосовується надзвичайно широкий спектр технічних засобів розвідки. Найбільш доступними залишаються засоби фіксації акустичних хвиль у вільному просторі. До них належать сучасні цифрові диктофони та закладні пристрої, які встановлюються приховано всередині приміщення. Сучасні акустичні радіозакладки мають мініатюрні розміри, можуть маскуватися під елементи інтер’єру або офісну техніку та передавати сигнал на приймач зловмисника по радіоканалу, інфрачервоному каналу або навіть через мережу Wi-Fi.

Для дистанційного перехоплення мови в приміщеннях з відкритими вікнами застосовуються спрямовані мікрофони. Їхня ефективність базується на формуванні спрямованої дії, що дозволяє уникати стороніх шумів та підсилювати корисний сигнал, який надходить з конкретного напрямку. За ідеальних погодних умов такі комплекси здатні забезпечити розбірливість мови на відстанях від 50 до 150 метрів, хоча міська забудова та фоновий шум суттєво знижують цей показник.

Значно серйознішу загрозу для захищених приміщень становлять засоби віброакустичної розвідки, зокрема електронні стетоскопи. Це спеціалізовані прилади контактного типу, призначені для перехоплення мовних сигналів крізь огороджувальні конструкції та інженерні комунікації. Основою таких пристроїв є високочутливі п’єзоелектричні акселерометри або контактні мікрофони, які перетворюють механічні мікровібрації твердих тіл, викликані акустичним тиском, в електричні сигнали. Головною перевагою сучасних стетоскопів є наявність блоку попередньої обробки сигналу, що включає малошумні підсилювачі та набір смугових фільтрів. Це дозволяє оператору відокремлювати мовний спектр частот та ефективно приглушувати завади низької частоти, наприклад, гул від роботи ліфтів чи транспорту. Завдяки такій обробці електронні стетоскопи здатні

зчитувати сигнали крізь бетонні та цегляні стіни товщиною понад 20см, а також використовувати труби водопостачання як провідники звуку на значні відстані в межах будівлі.

Для перехоплення інформації електромагнітними каналами ПЕМВН застосовуються засоби радіо та радіотехнічної розвідки. До цього класу належать скануючі приймачі та аналізатори спектра. Сучасні портативні аналізатори дозволяють не лише виявляти факт наявності випромінювання на певній частоті, але й записувати широкосмуговий сигнал для подальшого цифрового аналізу. Використовуючи спеціалізоване програмне забезпечення для обробки сигналів, зловмисник може виділити з радіошуму корисну інформацію, наприклад, відновити відеозображення з перехопленого сигналу або декодувати натискання клавіш бездротової клавіатури. Важливою особливістю цих засобів є їх пасивний режим роботи - вони нічого не випромінюють, тому виявити факт перехоплення технічними засобами захисту неможливо.

Засоби візуально-оптичного спостереження використовуються як засоби прямого візуального спостереження, до них належать: біноклі, телескопи, монокуляри та довгофокусні об'єктиви фото і відеокамер. Головною метою їх використання є отримання деталізованого зображення об’єктів з безпечної відстані. Завдяки високій кратності збільшення, такі засоби дозволяють зловмисникам вести спостереження за екранами моніторів через вікна, читати текстові документи на робочих столах та розпізнавати зміст розмов за артикуляцією губ співрозмовників, не наближаючись до контрольованої зони.

До оптико-електроних засобів відносять прилади нічного бачення та тепловізійні комплекси. Тепловізори, що працюють у дальньому інфрачервоному діапазоні, дозволяють виявляти місця прокладання кабельних трас в стінах або фіксувати роботу обладнання, що знаходиться в режимі очікування.

Найбільш небезпечним засобом є лазерні акустичні системи розвідки. Вони складаються з лазерного випромінювача та оптичного приймача. Такі системи дозволяють дистанційно зчитувати вібрацію віконного скла з відстані у сотні

метрів, забезпечуючи високу якість відновленого звуку без необхідності проникнення в контрольовану зону.

Висновки до першого розділу

У першому розділі здійснено теоретико-методологічний аналіз засад технічного захисту інформації. Визначено двобічну природу інформації як об’єкта захисту, де вона виступає одночасно стратегічним активом і джерелом потенційних ризиків. Встановлено, що ТЗІ є фундаментом загальної системи інформаційної безпеки, спрямованим на створення фізичних бар’єрів для унеможливлення витоку даних. Систематизовано понятійний апарат згідно з чинними національними стандартами. Виділено специфіку української нормативної доктрини, яка базується на пріоритеті захисту фізичного середовища та ставить перед системою захисту жорстку вимогу унеможливлення витоку, на відміну від імовірнісного підходу мінімізації ризиків. Проведено аналіз нормативно-правової бази, який виявив існування двох контурів регулювання: обов'язкового національного, що регламентує захист державних ресурсів, та гармонізованого міжнародного, що базується на властивостях інформації. Розроблено класифікацію загроз безпеці інформації. Визначено, що для цілей технічного захисту пріоритетним є поділ загроз за фізичним середовищем поширення. Це дозволило ідентифікувати основні технічні канали витоку як головний об’єкт подальшого дослідження.

Також проведений аналіз фізичних основ утворення технічних каналів витоку інформації дозволяє стверджувати, що сучасний об’єкт інформаційної діяльності перебуває під постійною загрозою з боку комплексних засобів технічної розвідки.

Виявлено, що витік інформації можливий не лише через очевидні акустичні канали, але й через приховані фізичні процеси: вібрацію будівельних конструкцій, побічні електромагнітні випромінювання цифрових інтерфейсів та модуляцію світлового потоку.

Встановлено, що кожен з цих каналів має чітку фізичну природу, що дозволяє застосовувати інструментальні методи для їх виявлення та вимірювання параметрів. Це створює методичну базу для проведення експериментальних

досліджень захищеності конкретного виділеного приміщення, результати яких будуть представлені у наступному розділі.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ НА ОІД

2.1 Генеральний план ОІД

Об’єктом дослідження є виділене приміщення, яке призначене для проведення нарад, конференцій та обміну мовною інформацією з обмеженим доступом між представниками керівного складу підприємства.

Приміщення розташоване на першому поверсі будівлі. Загальна площа приміщення складає 78 квадратних метрів, висота стелі дорівнює 2,4м. Щодо топологічного розміщення об’єкта відносно інших зон, то одна стіна є фасадною і виходить на внутрішнє подвір’я підприємства, яке є контрольованим, але відкритою територією. Три інші стіни межують із суміжними службовими кабінетами, які не входять до складу виділеного приміщення, проте знаходяться в межах контрольованої зони будівлі.

Інженерний захист та звукоізоляція приміщення визначаються характеристиками його огороджувальних конструкцій. Стіни приміщення виконані з монолітного залізобетону товщиною 200мм. Стеля виконана із залізобетонних плит перекриття стандартної конструкції, а підлога являє собою залізобетонну основу, покриту керамічною плиткою.

У приміщенні наявні два віконні отвори розміром 1500х1500мм, розташовані у зовнішній стіні, що виходить у внутрішній двір. Висота підвіконня від рівня підлоги становить 0,8м. Вікна металопластикові, подвійні. Для захисту від візуально-оптичного спостереження ззовні, вікна додатково обладнані ролетами.

Вхід до приміщення організовано через одні двері розміром 1400х2100мм. Двері металопластикові двостулкові з подвійним армованим склом, що забезпечує підвищену механічну міцність та знижує амплітуду коливань поверхні скла під дією акустичної хвилі. Доступ до приміщення суворо обмежений організаційними заходами та наявною системою контролю доступу.

Опалювальні прилади (радіатори) розташовані у нішах під кожним з двох вікон, а труби системи опалення проходять крізь перекриття та стіни до суміжних приміщень.

Для забезпечення повітрообміну у приміщенні встановлена система вентиляції. Металеві короби повітроводів проходять крізь зовнішню стіну та з’єднані із загальною системою вентиляції.

Освітлення здійснюється лампами денного світла. Електромережа приміщення підключена до загальної електрощитової будівлі, а лінії електроживлення виходять за межі контрольованої зони. Генеральний план ОІД схематично зображено на рис. 2.1

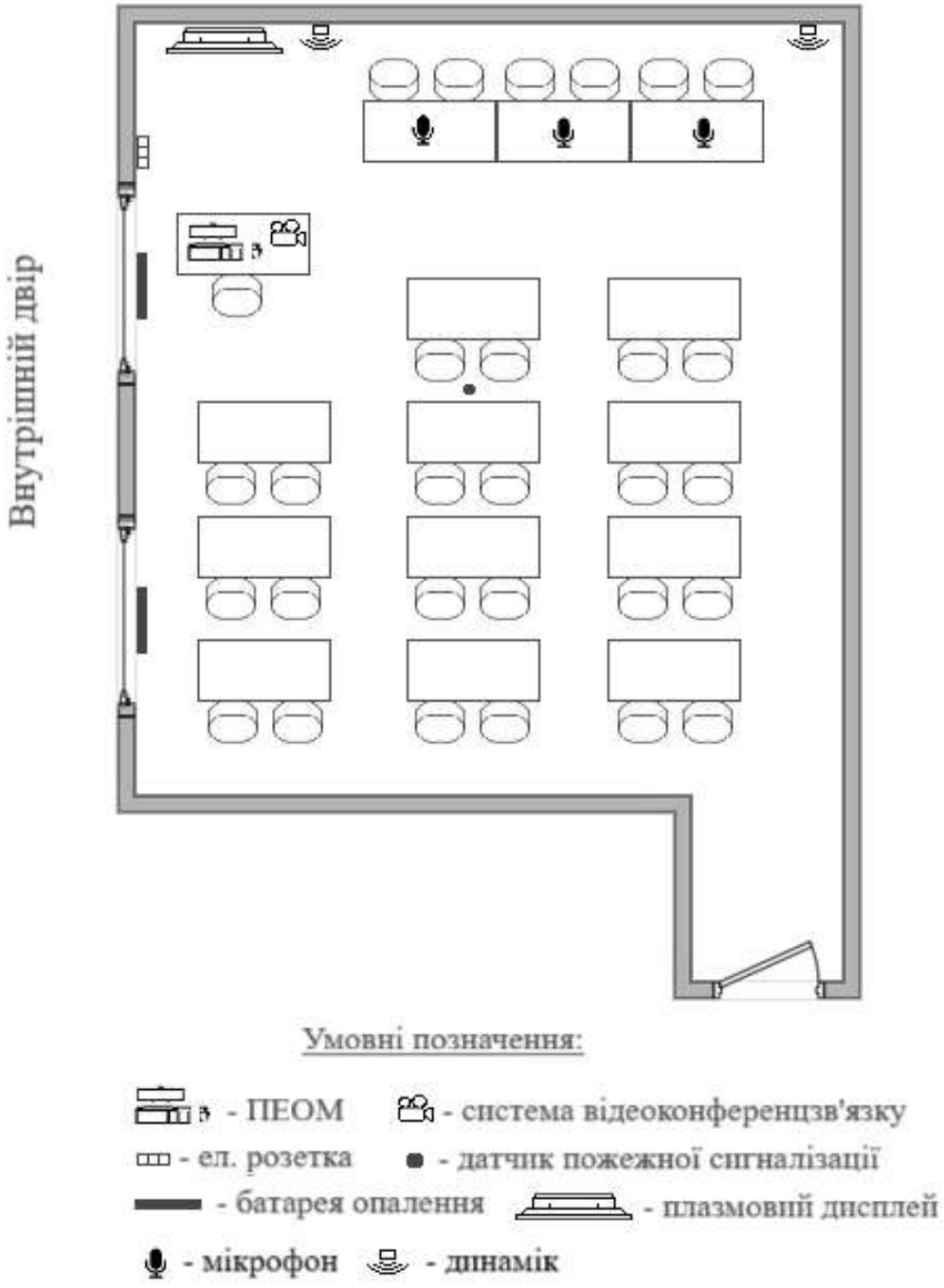

Рис. 2.1 Генеральний план ОІД

У приміщенні наявні лінії передачі даних, Ethernet, підключені до глобальної мережі Інтернет, що виходять за межі контрольованої зони. Також приміщення обладнано датчиками пожежної сигналізації, які з'єднані дротовою лінією з центральним пультом охорони.

Технічне забезпечення приміщення реалізовано на базі автоматизованого робочого місця, доповненого периферійним обладнанням для прийому та передачі інформації. Центральним елементом системи обробки інформації є ноутбук, який виконує роль керування відеоконференцзв'язком. Пристрій має активне підключення до глобальної мережі Інтернет, що забезпечує комутацію з віддаленими абонентами. Управління програмним забезпеченням та інтерфейсом конференції здійснюється оператором за допомогою комп'ютерної миші.

Система візуалізації інформації побудована на базі телевізійної панелі, яка підключена до ноутбука та слугує засобом відображення відеопотоку від учасників конференції, а також демонстрації презентаційних матеріалів, графіків та документів під час нарад.

Акустичне середовище приміщення організовано каналами відтворення: дві настінні колоноки, для забезпечення рівномірного звукового поширення. Вони отримують аудіосигнал безпосередньо від ноутбука та транслюють мову віддалених учасників конференції. Та канал мовного вводу: три настільні мікрофони, які розміщені безпосередньо перед керівниками на головному столі. Це дозволяє здійснювати якісне захоплення мовних сигналів присутніх осіб для їх подальшої передачі по каналу зв'язку.

Захоплення відеозображення у приміщенні здійснюється за допомогою спеціалізованої системи відеоконференцзв'язку, яка включає камеру високої чіткості. Система з'єднана з ноутбуком та спрямована на зону головного столу.

Перелік технічних засобів, розміщених на ОІД наведено в табл. 2.1.

Таблиця 2.1

Перелік ТЗ на ОІД

№	Найменування технічного засобу	Тип
1	Ноутбук 1шт.	Dell Latitude 3520
2	Комп’ютерна миша 1шт.	Logitech B100
3	Система відеоконференцзв'язку 1шт.	Logitech Group Video Conferencing System (960-001057)
4	Телевізор для виведення конференції 1шт.	Xiaomi TV A Pro
5	Настінні колонки 2шт.	SKY SOUND NSB-30B
6	Мікрофон 3шт.	REAL-EL MC-20
7	Датчики диму 1шт.	СПД-3

Таким чином, у приміщенні сформовано замкнуту систему обробки акустичної та візуальної інформації, центром якого є ноутбук, а середовищем поширення сигналів виступають дротові з’єднання між периферійними пристроями та комп’ютером.

2.2 Характеристика і опис технічних каналів витоку ОІД

У досліджуваному приміщенні площею 78 квадратних метрів, призначеному для конференцій керівного складу, циркулює мовна інформація з обмеженим доступом, а також здійснюється обробка даних за допомогою технічних засобів. Наявність у залі комплексу обладнання для обробки інформації у поєднанні з архітектурними особливостями першого поверху, формує складну систему потенційних каналів витоку інформації [16-23].

Першочерговою загрозою є акустичний канал, який може реалізуватися через недостатню звукоізоляцію огороджувальних конструкцій. Незважаючи на наявність металопластикових дверей з подвійним армованим склом, зона притулу та монтажні шви залишаються вразливими місцями для прямого прослуховування з коридору. Крім того, серйозну небезпеку становить система вентиляції: металеві

короби повітроводів, що проходять крізь зовнішню стіну, можуть діяти як хвилеводи, виводячи акустичні сигнали за межі контрольованої зони. Також, враховуючи розташування вікон у бік внутрішнього двору, існує ризик підслуховування з меж контрольованої зони без застосування технічних засобів, або застосування спрямованих мікрофонів з прилеглої території у випадках, коли вікна або ролети відкриті під час нарад.

Віброакустичний канал витоку інформації на даному об’єкті утворюється внаслідок впливу акустичного поля на будівельні конструкції та інженерні комунікації. Стіни з монолітного залізобетону частично гасять коливання, проте слабкими ланками є віконні склопакети та система опалення. Труби радіаторів, розташованих під вікнами, проходять крізь перекриття та стіни до суміжних приміщень, що дозволяє зловмиснику, який має доступ до цих приміщень, встановити контактні вібродатчики на трубах і знімати мовну інформацію. Значна площа скління також сприяє перетворенню звукових хвиль у вібрацію скла, що робить можливим використання лазерних акустичних систем розвідки. З огляду на розміщення об’єкта на першому поверсі, кути опромінення вікон з боку внутрішнього двору є сприятливими для таких атак.

Суттєво підвищує ризики наявність у приміщенні технічних засобів для переговорів, які реалізовано на базі автоматизованого робочого місця, центральним елементом якого є ноутбук з доступом до мережі Інтернет. Введення аудіовізуальної інформації здійснюється через спеціалізовану периферійну систему відеоконференцзв’язку, що виконує функцію концентратора сигналів. До складу цієї системи входять камера високої чіткості, орієнтована на зону наради, та масив із трьох настільних мікрофонів, які забезпечують зональне захоплення мови учасників. Зазначені засоби підключені безпосередньо до центрального блоку системи відеоконференцзв’язку. Комутація всієї системи з керуючим ноутбуком реалізована через єдиний інтерфейсний кабель USB. Виведення інформації здійснюється на телевізійну панель та настінні акустичні системи. Така архітектура формує єдиний цифровий потік даних від сенсорів до комп’ютера через послідовний інтерфейс.

Канали витоку за рахунок ПЕМВН на об’єкті обумовлені роботою ноутбука, телевізора, системи відеоконференцзв’язку та периферії. Під час обробки та виведення інформації на екран телевізора або монітор ноутбука виникають електромагнітні випромінювання, що несуть інформативні ознаки зображення та цифрових даних. Окремим джерелом критичних загроз є інтерфейсний кабель стандарту HDMI, що з’єднує ноутбук із телевізором та USB кабель, що з’єднує систему відеоконференцзв’язку з ноутбуком. Через високу частоту тактових імпульсів при передачі відеопотоку та значну довжину, кабелі виконують роль ефективної антени, що випромінює широкосмуговий сигнал із ознаками візуальної інформації.

Оскільки лінії електроживлення та мережі Ethernet виходять за межі контрольованої зони без гарантованого використання фільтрів, існує висока ймовірність наведення інформативних сигналів у цих мережах та їх подальшого перехоплення.

Додатковим фактором ризику є наявність системи відеоконференцзв’язку, підключеної до Інтернету, що створює загрозу несанкціонованого віддаленого підключення до камери та мікрофонів, перетворюючи легальний засіб зв’язку на інструмент розвідки.

Візуально-оптичний канал витоку залишається актуальним через наявність вікон на першому поверсі. Це дозволяє здійснювати спостереження за діями учасників наради, а також фіксувати зображення з екрана телевізора або монітора ноутбука, якщо вони повернуті до вікна. Загроза посилюється можливістю використання сучасної оптики з високою роздільною здатністю для зчитування документів на столі. Хоча наявність ролетів є ефективним заходом протидії, їх захисний потенціал реалізується лише за умови суворого дотримання організаційних процедур закриття вікон під час проведення конфіденційних заходів.

2.3. Дослідження віброакустичного каналу витоку ОІД

З метою практичної перевірки теоретичних припущень щодо вразливості огороджувальних конструкцій, проведемо серію інструментально-розрахункових досліджень.

2.3.1. Методологія дослідження

В основі методики лежить інструментально-розрахунковий формантний метод оцінки, регламентований НД ТЗІ 2.3-017-08 «Методика контролю захищеності мовної інформації від витоку акустичним та віброакустичним каналами»[12]. Ключовим фізичним параметром є відношення сигнал/шум (SNR), що розраховується в п’яти октавних смугах частот (250, 500, 1000, 2000, 4000 Гц). На його основі обчислюється інтегральний індекс артикуляції (R) за формулою:

$$R = \sum_{i=1}^{5} W_i L_i \qquad (2.1)$$

де W_i - вагові коефіцієнти значущості кожної октавної смуги для розбірливості мови, а L_i - коефіцієнт сприйняття, що є функцією від SNR в цій смузі:

$$L_i = \begin{cases} 0, & SNR_i \leq -15\text{дБ} \\ \dfrac{SNR_i + 15}{30}, & -15\text{дБ} < SNR_i < +15\text{дБ} \\ 1, & SNR_i \geq +15\text{дБ} \end{cases} \qquad (2.2)$$

Далі, за допомогою стандартних емпіричних кривих, значення індексу артикуляції R перераховується в кінцевий критерій - словесну розбірливість (W, %).

2.3.2. Монолітна стіна

Для проведення дослідження було змодельовано експериментальний стенд, що відтворює реальні умови проведення конференції. Першим об’єктом дослідження виступала огороджувальна конструкція - монолітна залізобетонна стіна товщиною 200 мм, що межує з контрольованою територією. Всередині приміщення розміщується джерело тестового сигналу (рожевий шум з рівнем звукового тиску 70 дБ), що відповідає середнім параметрам гучної мови під час нарад. Вимірювання рівнів віброприскорення сигналу (L_s) та завади (L_n)

проводяться на зовнішній поверхні стіни за допомогою прецизійного акселерометра SV 80 та аналізатора спектра SVANTEK SVAN 977.

При описаному дослідженні вдалося зняти показники рівнів завад та сигналу за допомогою аналізатора SVAN 977 та для відображення їх занесено у графік, побудований за результатами вимірювань (рис.2.2).

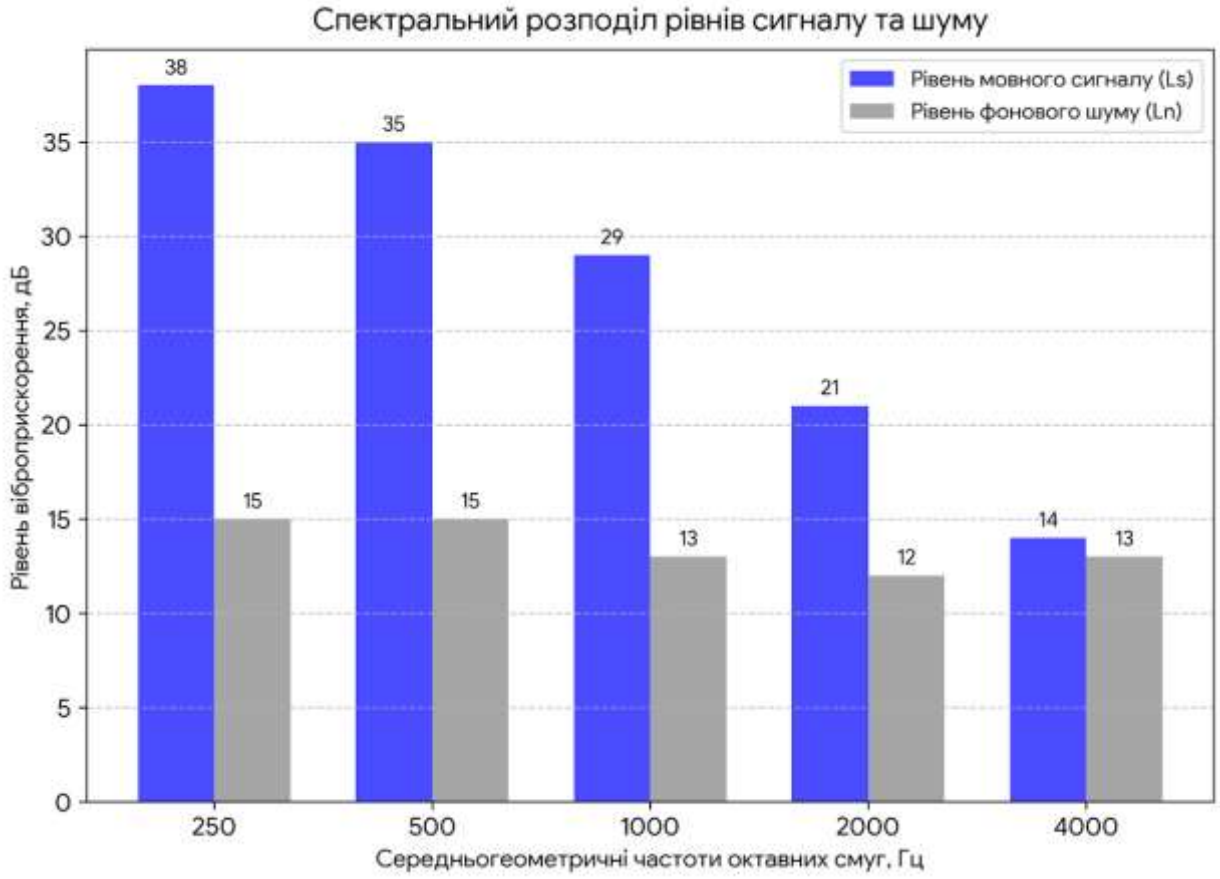

Рис. 2.2 Спектральний склад віброакустичного сигналу на зовнішній поверхні стіни

Далі згідно отриманих значень рівнів сигналу L_s та рівнів завад L_n обраховується відношення сигналу/шуму SNR в кожній октавній смузі частот, їх сумою. За формулою (2.2) обраховуємо коефіцієнт сприйняття L_i. Вагові коефіцієнти W_i є табличними константами для визначених октавних смуг частот, які визначені в нормативному документі НД ТЗІ 2.3-017-08. Для зручності обрахунків данні записані у таблицю 2.2.

Таблиця 2.2

Вимірювання значень досліду стіни

Частота, Гц	Рівень сигналу, L_s (дБ)	Рівень завади, L_n (дБ)	Відношення сигнал/шум, SNR (дБ)	Вагові коефіцієнти, W_i	Коефіцієнт сприйняття, L_i
250	38	15	+23	0.113	1.00
500	35	15	+20	0.205	1.00
1000	29	13	+16	0.207	1.00
2000	21	12	+9	0.275	0.80
4000	14	13	+1	0.200	0.53

Обрахунки коефіцієнтів сприйняття в яких значення SNR лежить у межах (-15дБ; +15дБ):

$$L_{i2000} = \frac{(9+15)}{30} = 0.8, \qquad L_{i4000} = \frac{(1+15)}{30} = 0.533;$$

Розрахунок індексу R:

$$R = 0.113 + 0.205 + 0.207 + (0.275 * 0.80) + (0.200 * 0.53) = 0.85$$

Отримане значення інтегрального індексу артикуляції R = 0.85 згідно з графіком переведення у словесну розбірливість відповідає $W \approx 97\%$ (рис.2.3).

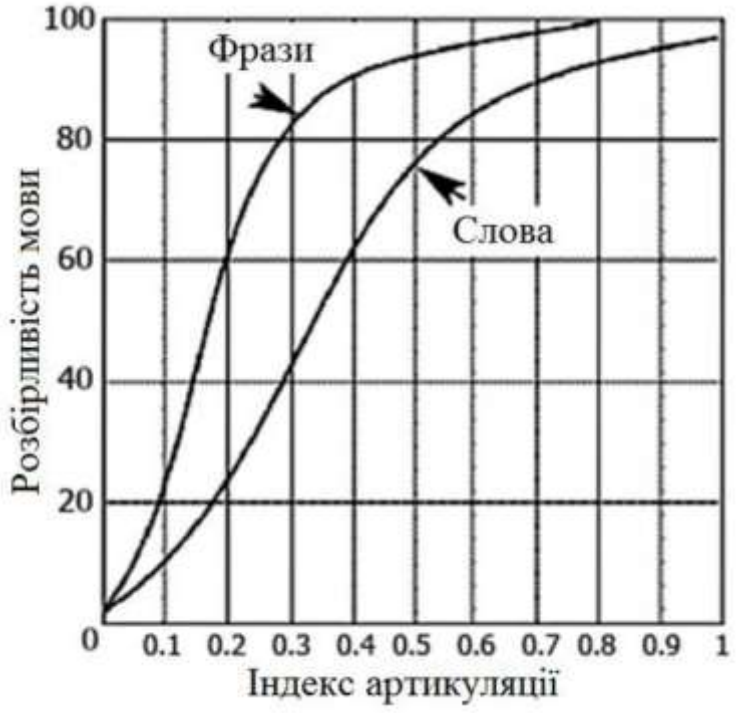

Рис.2.3 Залежність індексу артикуляції від розбірливості мови

Що свідчить про небезпеку витоку віброакустичного каналу інформації через монолітну стіну.

2.3.3. Віконна рама

Окремим етапом експериментальних досліджень стала оцінка захищеності мовної інформації через світлопрозорі огороджувальні конструкції - віконні рами. Враховуючи фізичні характеристики скла, мала поверхнева щільність та висока пружність, цей канал витоку вважається найбільш небезпечним.

Вимірювання рівнів віброприскорення, проведені на поверхні скла показали значне перевищення рівня тестового сигналу над фоновими шумами (рис. 2.4).

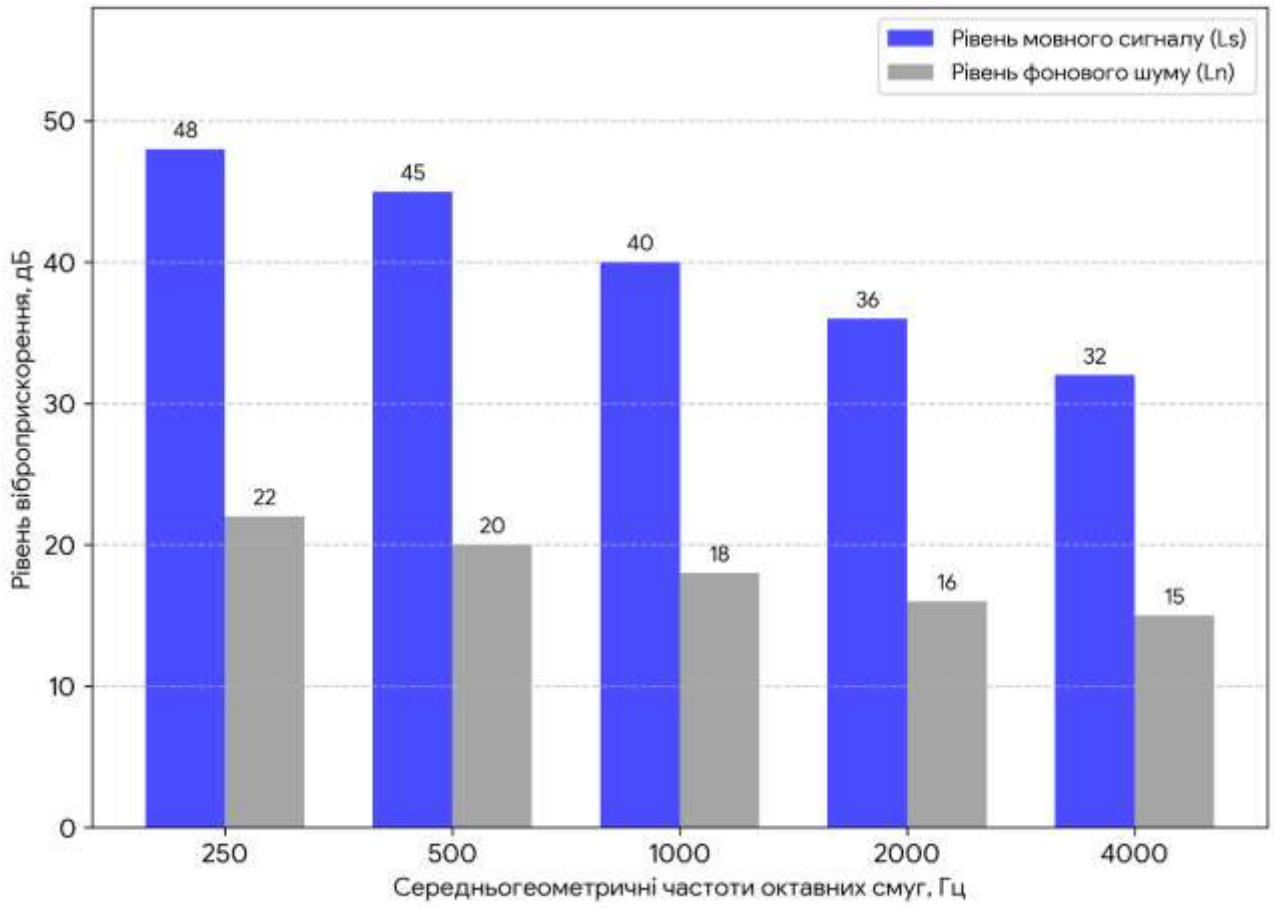

Рис. 2.4 Спектральний склад віброакустичного сигналу на поверхні скла

Зокрема, у низькочастотному діапазоні 250 Гц рівень сигналу досягав 48 дБ при рівні шуму 22 дБ, що забезпечило відношення сигнал/шум на рівні +26 дБ.

В ході розрахунків встановлено, що у всіх контрольованих октавних смугах частот значення SNR перевищує пороговий рівень насичення (+15 дБ), внаслідок чого коефіцієнт сприйняття L_i дорівнює одиниці. Результати занесенні у табл 2.3

Таблиця 2.3

Вимірювання значень досліду вікна

Частота, Гц	Рівень сигналу, L_s (дБ)	Рівень завади, L_n (дБ)	Відношення сигнал/шум, SNR (дБ)	Вагові коефіцієнти, W_i	Коефіцієнт сприйняття, L_i
250	48	22	+26	0.113	1.00
500	45	20	+25	0.205	1.00
1000	40	18	+22	0.207	1.00
2000	36	16	+20	0.275	1.00
4000	32	15	+17	0.200	1.00

Розрахунок індексу R:

$$R = 0.113 + 0.205 + 0.207 + 0.275 + 0.200 = 1.00$$

Отриманий інтегральний індекс артикуляції склав $R = 1.00$, що згідно з нормативними методиками відповідає словесній розбірливості $W = 100\%$,. Це свідчить про те, що звичайний склопакет без застосування засобів активного віброакустичного зашумлення не створює достатнього опору для унеможливлення перехоплення мовної інформації, дозволяючи повністю відновити зміст розмови.

2.3.4. Система опалювання

Останнім досліджуваним елементом віброакустичного каналу витоку стала інженерна комунікація, що виходить за межі контрольованої зони - система центрального опалення. Враховуючи високу акустичну провідність металу та хвилевідні властивості труб, цей канал може забезпечувати передачу мовного сигналу на значні відстані з мінімальним затуханням.

Вимірювання проводились безпосередньо на металевій поверхні радіатора опалення. Для забезпечення надійного акустичного контакту акселерометра з криволінійною поверхнею використовувався спеціалізований магнітний адаптер. Результати вимірювань зафіксували високі рівні віброприскорення корисної

складової сигналу, особливо в області низьких та середніх частот (250–1000 Гц), де метал найбільш схильний до резонансних явищ (рис. 2.5).

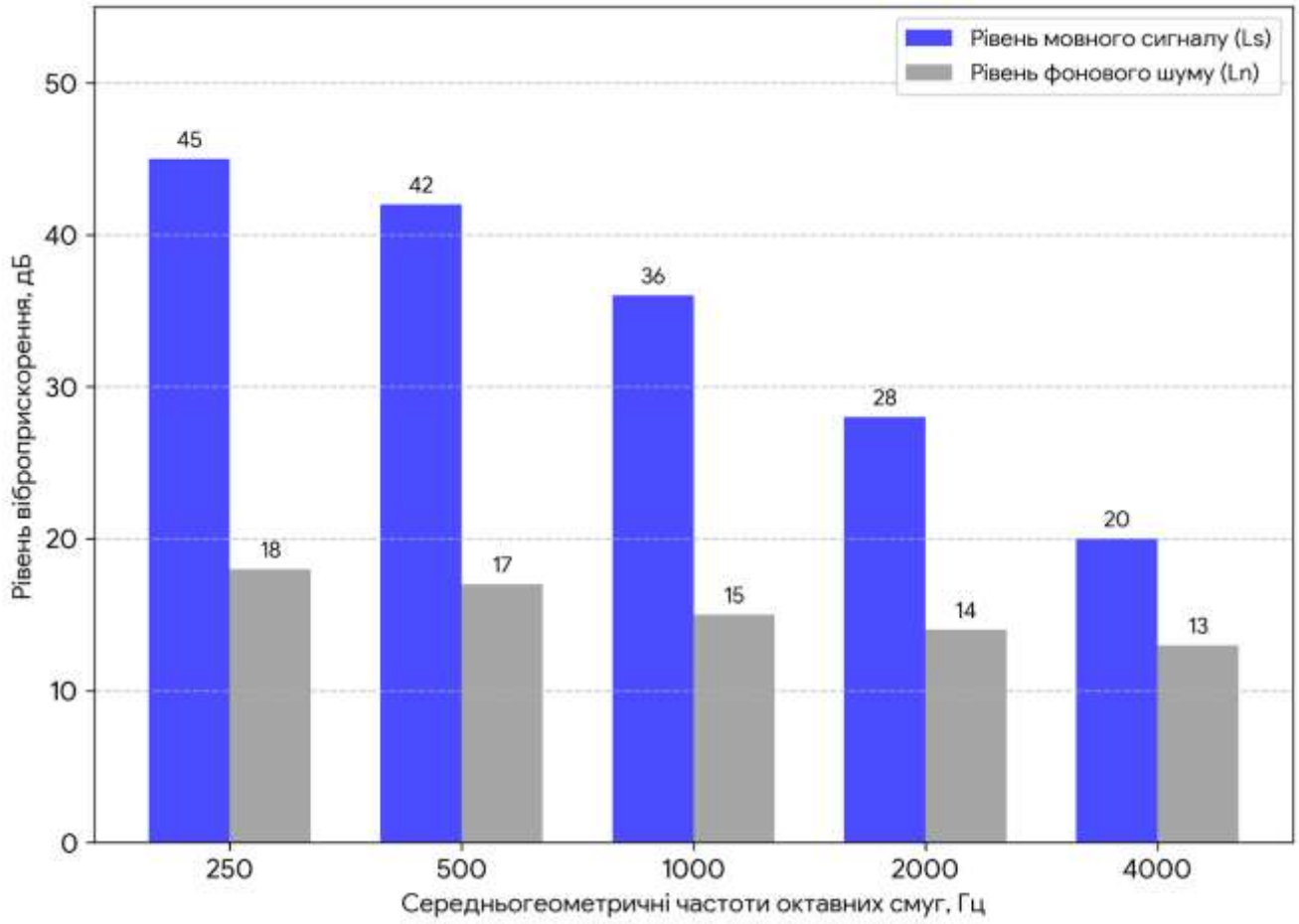

Рис. 2.5 Спектральний склад віброакустичного сигналу на поверхні радіатора

Занесемо ці результати у таблицю 2.4, та продовжимо обрахунки індексу артикуляції.

Таблиця 2.4

Вимірювання значень досліду радіатора

Частота, Гц	Рівень сигналу, L_s (дБ)	Рівень завади, L_n (дБ)	Відношення сигнал/шум, SNR (дБ)	Вагові коефіцієнти, W_i	Коефіцієнт сприйняття, L_i
250	45	18	+27	0.113	1.00
500	42	17	+25	0.205	1.00
1000	36	15	+21	0.207	1.00

Продовження табл. 2.4

2000	28	14	+14	0.275	0.97
4000	20	13	+7	0.200	0.73

Обрахунки коефіцієнтів сприйняття в яких значення SNR лежить у межах (-15дБ; +15дБ):

$$L_{i2000} = \frac{(14+15)}{30} = 0.967, \qquad L_{i4000} = \frac{(7+15)}{30} = 0.733,$$

Розрахунок індексу R:

$$R = 0.113 + 0.205 + 0.207 + (0.275 * 0.97) + (0.200 * 0.73) = 0.938 \approx 0.94$$

Розрахований індекс артикуляції склав $R = 0.94$, що відповідає майже повній 99% словесній розбірливості. Деяке зниження коефіцієнта сприйняття на високих частотах (4000 Гц) викликане опором рідини, яка поглинає вібрацію, проте це суттєво не впливає на загальну розбірливість мови. Отримані дані підтверджують, що металеві комунікації потребують обов'язкового захисту.

2.4. Дослідження електромагнітного каналу витоку на ОІД

Окремим і критично важливим етапом дослідження захищеності ОІД є аналіз каналів витоку за рахунок ПЕМВН [13]. В умовах сучасної кімнати перемовин основним джерелом небезпечних сигналів є відеовідображувальна система, зокрема інтерфейс передачі відеоданих від ноутбука до демонстраційного екрана телевізора. Для передачі відеопотоку високої чіткості використовується інтерфейс HDMI. Фізика передачі сигналу в цьому стандарті базується на технології Transition Minimized Differential Signaling (TMDS), що передбачає передачу високочастотних цифрових імпульсів. Як випливає з теорії радіотехнічних кіл та сигналів і зазначається у фаховій літературі [9], цифрові відеосигнали, що за своєю формою наближені до прямокутних імпульсів, мають широкий спектр вищих гармонік. Ці високочастотні складові, згідно з законами електродинаміки, ефективно випромінюються провідниками інтерфейсів у навколишній простір, створюючи канал витоку інформації.

З’єднувальний кабель HDMI, що прокладений від нутбуку до настінного телевізора, має значну довжину, понад 2 метри, і за відсутності якісного екранування виконує роль ефективної передавальної антени.

Для підтвердження наявності небезпечного випромінювання було проведено інструментальний контроль радіоефіру з допомогою портативного аналізатору спектра tinySA Ultra, налаштований на діапазон частот 0–400 МГц. з телескопічною антеною на відстані 2-3 см. до кабелю.

Фіксація результатів вимірювань здійснювалася за допомогою спеціалізованого програмного забезпечення tinySA App. Дане програмне забезпечення дозволяє підключити аналізатор спектру до персонального комп’ютера через інтерфейс USB, що забезпечує візуалізацію спектрограми на моніторі ПК у реальному часі та дозволяє зберігати графічні дані високої чіткості для подальшого аналізу.

У ході сканування радіочастотного спектра було зафіксовано появу стійких вузькосмугових сигналів, які відсутні при вимкненому джерелі відеосигналу. Результати вимірювань демонструються на графіку у вигляді спектрограми (рис. 2.6).

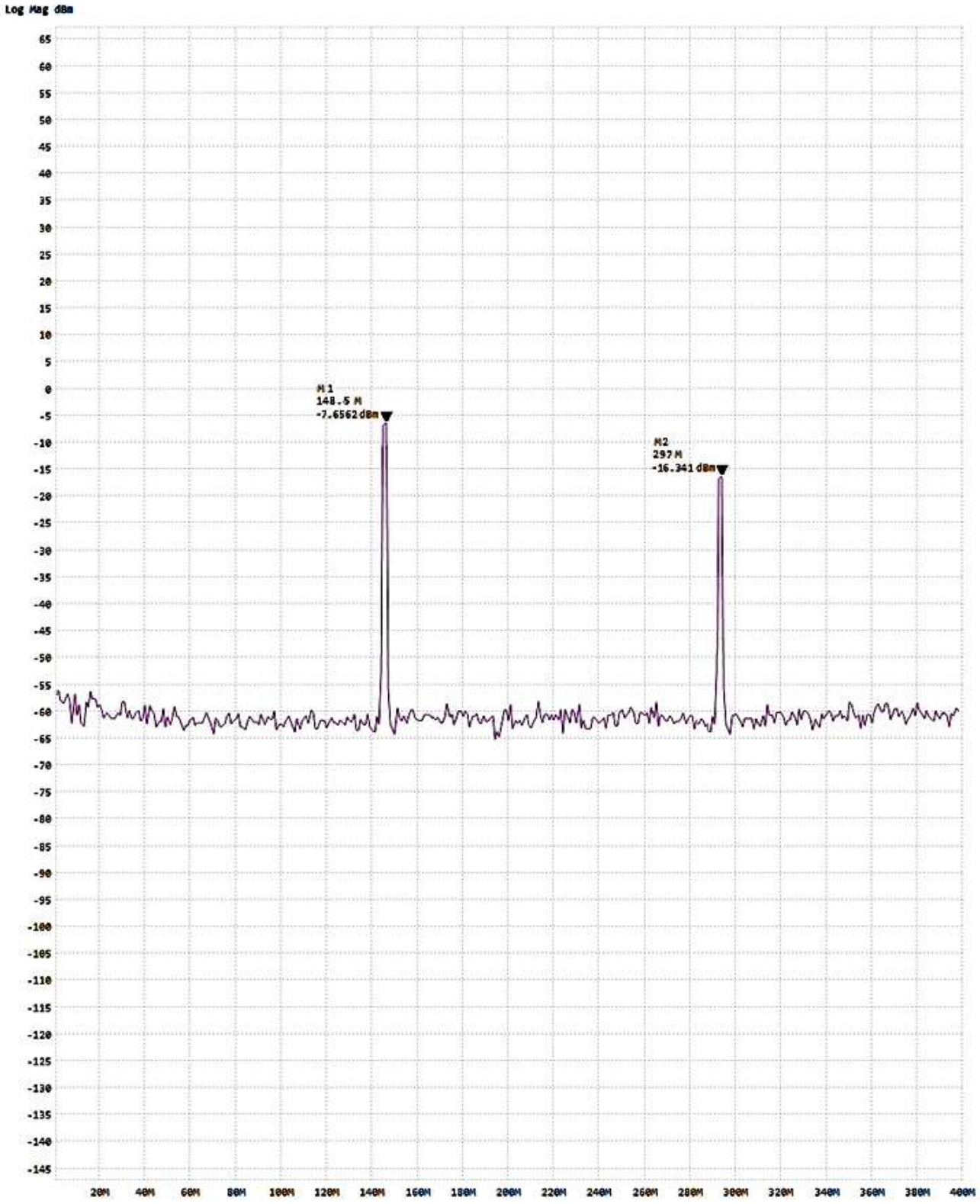

Рис. 2.6 Спектрограма випромінювання інтерфейсного кабелю HDMI

Аналіз спектрограми дозволяє виділити характерні інформативні ознаки перехопленого сигналу:

- Маркер 1: Основна гармоніка на частоті 148.5 МГц зафіксовано потужний сплеск сигналу з амплітудою -7.7 dBm. Частота 148.5 МГц

точно відповідає тактовій частоті пікселізації для відеорежиму 1080p при 60 Гц. Це є прямим доказом того, що джерелом випромінювання є саме відеоінтерфейс. Рівень фонового шуму становить приблизно -60 dBm. Таким чином, перевищення корисного сигналу над шумом складає 53 дБ. Це критично високий показник, який дозволяє перехоплювати сигнал на значній відстані, до 10-15 метрів, навіть за межами приміщення.

- Маркер 2: Друга гармоніка на частоті 297.0 МГц спостерігається друга гармоніка сигналу з рівнем -16.3 dBm. Наявність чітких гармонік полегшує задачу відновлення зображення засобами спецтехніки, наприклад, методом растрової розгортки.

Далі необхідно оцінити захищеність каналу передачі даних системи відеоконференцзв'язку. Наявна система виконує роль концентратора, який об'єднує відеопотік високої чіткості від камери та аудіосигнали від масиву мікрофонів у єдиний цифровий потік. Для передачі цього масиву даних на керуючий ноутбук використовується послідовний інтерфейс USB 2.0. USB-кабель довжиною близько 1 метру, що з'єднує блок ВКЗ з ноутбуком, також виступає в ролі антени, що випромінює модульований інформативний сигнал.

Враховуючи частотні характеристики інтерфейсу USB, прилад було залишено в діапазоні частот 0–400 МГц, а вимірювальна антена розміщувалася в безпосередній близькості до з'єднувального кабелю системи.

У ході сканування, при активному режимі відеоконференції, було зафіксовано появу характерних сплесків амплітуди, які суттєво зменшуються при припиненні передачі даних. Результати вимірювань демонструються на графіку у вигляді спектрограми (рис 2.7).

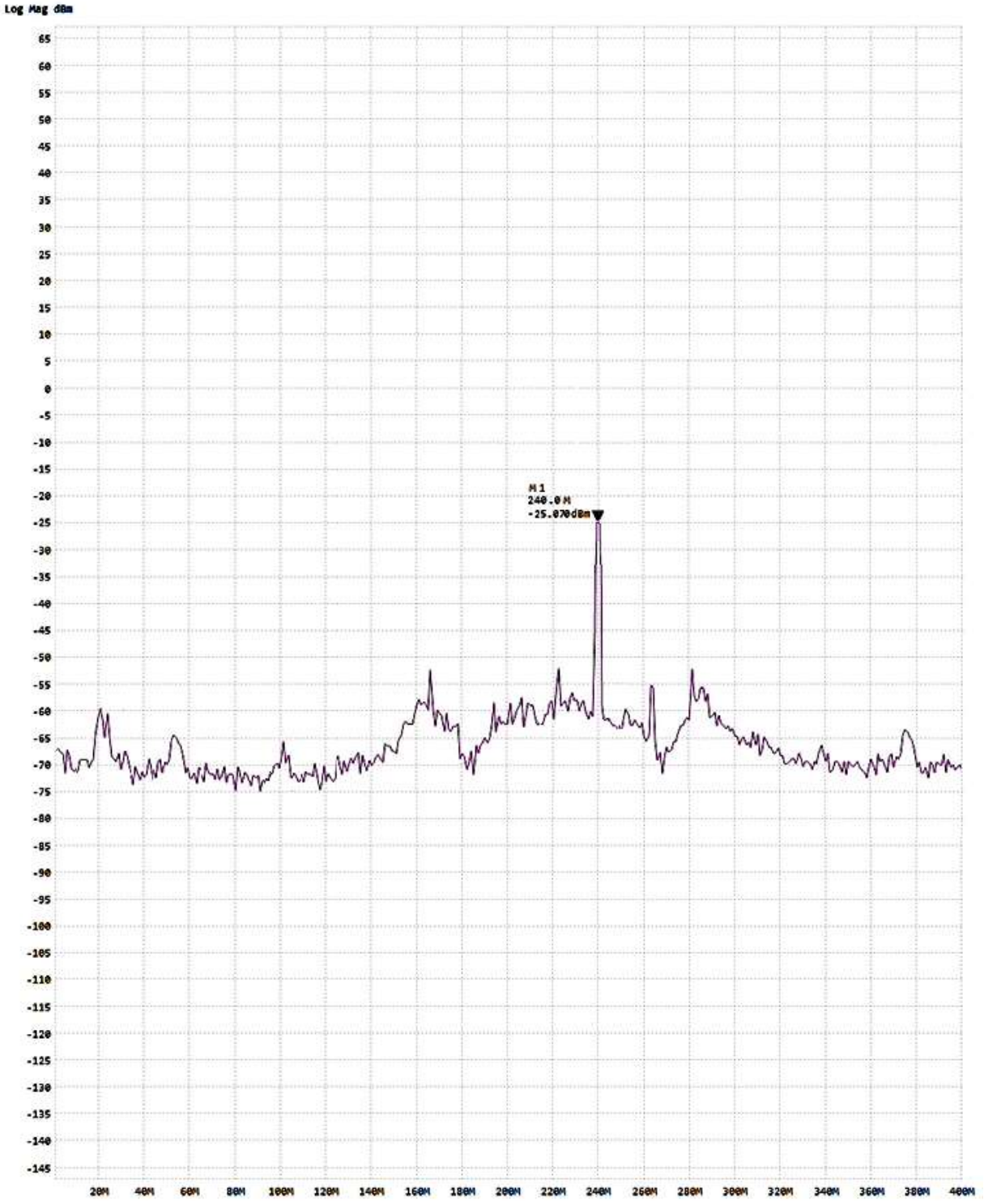

Рис. 2.7 Спектрограма випромінювання інтерфейсного кабелю USB

Спектрограма демонструє маркер 1 на частоті 240.0 МГц зафіксовано найбільш потужний сплеск сигналу з амплітудою -25.1 dBm. Дана частота є фундаментальною для стандарту USB 2.0 High Speed і відповідає половині тактової частоти шини передачі даних. Це підтверджує, що джерелом випромінювання є саме інтерфейсний кабель, по якому транслюється сумарний потік аудіо та

відеоінформації. При рівні фонового шуму близько -65 dBm, перевищення сигналу над шумом складає 40 дБ. Таке співвідношення сигнал/шум є критичним і свідчить про високу ймовірність перехоплення комбінованої інформації засобами радіорозвідки.

Проведене дослідження підтвердило, що стандартний кабель HDMI є джерелом інтенсивного побічного електромагнітного випромінювання. Високий рівень сигналу на тактових частотах створює реальний канал витоку візуальної інформації. Залишати даний канал без захисту неприпустимо, оскільки це дозволяє зловмиснику проводити безконтактне знімання інформації з прилеглої території, внутрішнього двору.

Висновки до другого розділу

У другому розділі проведено комплексне дослідження ОІД, спрямоване на виявлення та інструментальну оцінку технічних каналів витоку мовної та візуальної інформації.

Аналіз інженерно-технічних особливостей об’єкта показав, що досліджуване приміщення, попри наявність базових огороджувальних конструкцій має низку критичних вразливостей. Розміщення на першому поверсі, наявність значної площі скління, що виходить у внутрішній двір, та транзитне проходження інженерних комунікацій, системи опалення та вентиляції, створюють сприятливі умови для несанкціонованого знімання інформації.

У ході моделювання загроз було ідентифіковано та схарактеризовано повний перелік потенційних технічних каналів витоку інформації. Встановлено, що найбільш небезпечними для даного ОІД є віброакустичний, акустичний та електромагнітний канал

Експериментальне дослідження віброакустичного каналу підтвердило недостатність пасивного захисту. Інструментальні вимірювання та подальші розрахунки за формантним методом показали критично високі значення словесної розбірливості мови на зовнішніх поверхнях без застосування засобів активного захисту:

- для огороджувальних конструкцій (стін): $W = 97\%$;

- для світлопрозорих конструкцій (вікон): $W = 100\%$;
- для системи опалення (труб радіаторів): $W = 99\%$.

Отримані показники підтверджують можливість повного відновлення змісту переговорів зловмисником за допомогою контактних вібродатчиків або лазерних акустичних систем.

Дослідження електромагнітного каналу виявило наявність потужного побічного електромагнітного випромінювання від інтерфейсних кабелів відеосистеми HDMI та USB. Спектральний аналіз зафіксував стійкі гармоніки тактової частоти пікселізації, рівень яких перевищує фоновий шум на 40–50 дБ. Це свідчить про те, що з’єднувальні лінії функціонують як передавальні антени, створюючи реальну загрозу дистанційного перехоплення та реконструкції відеозображення з екрана монітора чи відеокамери.

3 РЕКОМЕНДАЦІЇ ЩОДО ВДОСКОНАЛЕННЯ СИСТЕМИ ТЗІ

3.1. Впровадження системи активного віброакустичного захисту

Результати експериментальних досліджень, наведені у другому розділі, засвідчили, що пасивні властивості огороджувальних конструкцій не забезпечують достатнього рівня загасання акустичних сигналів. Показник словесної розбірливості мови на рівні $W = 97\%$ свідчить про наявність неконтрольованого каналу витоку інформації.

Для нейтралізації цієї загрози рекомендується впровадження системи активного акустичного захисту (САЗ), принцип дії якої полягає у створенні маскуючої шумової завади у твердих тілах: стінах, вікнах, трубах опалення. Ключовим елементом ефективності такої системи є правильний вибір виконавчих пристроїв - вібровипромінювачів.

Враховуючи різнорідність каналів витоку: скло, метал та бетон, застосування одного типу випромінювачів є технічно неможливим через різні резонансні властивості матеріалів. У зв’язку з цим, пропонується використання комбінації спеціалізованих перетворювачів серії PIAC[14, 15].

Скляні конструкції є специфічним середовищем поширення звуку. Скло має малу масу та високу добротність, що робить його чутливим до найменших акустичних коливань, але водночас вразливим до додаткового навантаження масою датчика. Тому найкраще підійде вібровипромінювач п’єзоелектричний PIAC-2ВП. Даний прилад виконаний на основі п'єзокерамічного елемента, що дозволило досягти малих габаритів та незначної маси, до 50 г. Таке технічне рішення є критично важливим для забезпечення узгодження мас, оскільки надто важкий датчик на склі працював би неефективно через інерцію та гасив би власні корисні коливання завади. П’єзоелектричний принцип дії забезпечує ефективну генерацію вібрацій у мовному діапазоні частот 250 Гц - 5000 Гц, що є необхідною умовою для протидії лазерним акустичним системам розвідки. Монтаж пристрою здійснюється за допомогою спеціального акустично клею, безпосередньо на поверхню скла, що гарантує надійний акустичний контакт без порушення цілісності склопакета.

Для захисту огороджувальних конструкцій та комунікацій доцільно використовувати РІАС-2ГС. Стіни з монолітного залізобетону, товщиною 200 мм, та сталеві труби опалення є масивними конструкціями з високим акустичним опором. Для збудження в них вібрації необхідного рівня розгойдування масиву бетону потрібне джерело значної механічної сили. Головним чинником вибору є висока потужність електромагнітної системи, яка генерує значне штовхаюче зусилля, здатне створити рівномірне поле завад у товщі залізобетону в радіусі 1,5-2,5 метра від точки кріплення. Важливою перевагою є універсальність кріплення, оскільки конструкція корпусу передбачає можливість жорсткого механічного монтажу. Для стін використовується кріплення за допомогою дюбеля, що забезпечує передачу вібрації в глибину моноліту, а для труб опалення - монтаж за допомогою металевих хомутів, що дозволяє ефективно передавати вібрацію на метал труби та блокувати канал витоку до суміжних приміщень.

Ефективність роботи системи активного віброакустичного захисту прямо залежить від рівномірності розподілу маскуючої завади по площі огороджувальних конструкцій. Для досліджуваного приміщення з розмірами 13х6м розроблено підрахунок кількості вібровипромінювачів з урахуванням радіусу їх ефективної дії та коефіцієнта загасання звуку в бетоні.

Захист світлопрозорих конструкцій, а саме двох віконних отворів розміром 1,5х1,5м забезпечується встановленням двох вібровипромінювачів типу РІАС-2ВП. Монтаж приладів здійснюється на геометричний центр склопакета або зі зміщенням на 1/3 діагоналі для уникнення вузлів стоячих хвиль, причому кріплення виконується на внутрішнє скло з боку приміщення. Основною метою даного заходу є створення хаотичних коливань поверхні скла для зриву модуляції лазерного променя.

Щодо захисту системи опалення, радіатори якої розташовані під кожним вікном, передбачено використання одного датчика типу РІАС-2ГС. Технологія монтажу передбачає кріплення датчика не на корпус батареї, щоб уникнути паразитного акустичного шуму в повітрі, а безпосередньо на металеву трубу у

місці її виходу зі стіни. Це дозволяє ефективно блокувати канал поширення звуку по металевих трубах до сусідніх приміщень.

Організація захисту огороджувальних конструкцій базується на розрахунку периметра приміщення, який складає 38 метрів. Для монолітного залізобетону товщиною 200 мм радіус ефективного перекриття одним датчиком РІАС-2ГС приймається рівним 2,5 м. Для забезпечення надійного захисту датчики розміщуються з кроком 3-4 метри, що гарантує перекриття зон їх дії. На кожній з довгих стін встановлюється по 3 датчики РІАС-2ГС, рівномірно розподілені по довжині з кроком приблизно 4,5 м. На коротких стінах достатньо встановити по 1 датчику по центру стіни, оскільки радіус дії перекриває всю її ширину. Загальна кількість випромінювачів для стін становить 8 одиниць. Висота монтажу обирається на рівні 30-50 см від підлоги.

Зведена специфікація виконавчих пристроїв САЗ, необхідних для обладнання приміщення, наведена в таблиці 3.1.

Таблиця 3.1

Специфікація засобів віброакустичного захисту

Об’єкт захисту	Тип випромінювача	Кількість, шт.	Тип кріплення
Вікна (1,5х1,5м)	РІАС-2ВП	2	На скло клейом
Труби опалення	РІАС-2ГС	1	Механічне хомутом
Стіни (периметр)	РІАС-2ГС	8	Анкерне
Всього		11	

Схему розміщення всіх спеціалізованих перетворювачів з урахуванням всіх описаних характеристик зображено на рисунку 3.1.

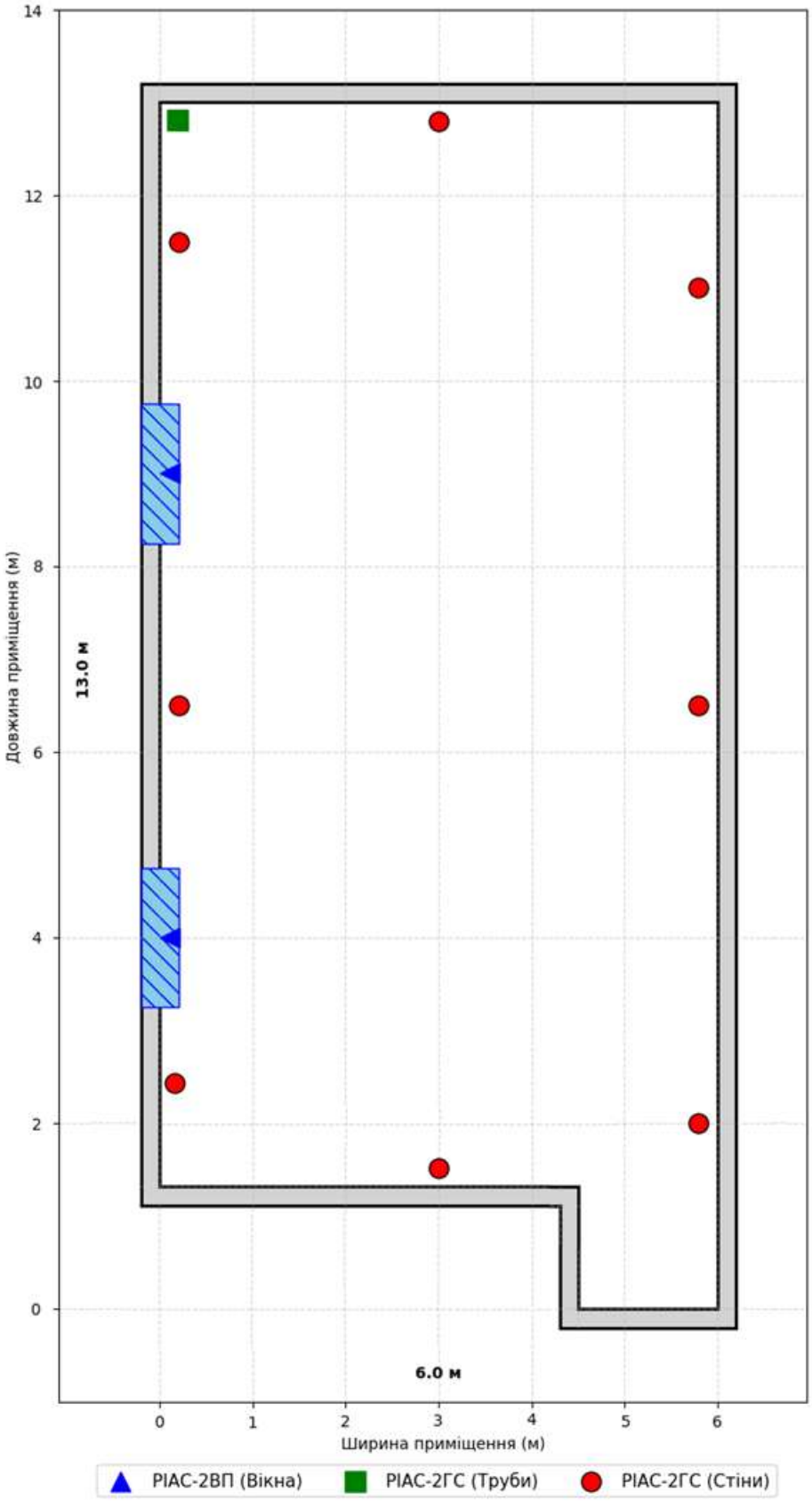

Рис. 3.1 Схема розміщення вібровипромінювачів САА3

Для проведення контрольного розрахунку змодельовано ситуацію, за якої система активного захисту функціонує в штатному режимі, генеруючи на огороджувальних конструкціях маскуючу заваду мовленнєвоподібного шуму. При цьому рівень акустичного тиску мовного сигналу всередині приміщення залишається незмінним, а рівень шуму на зовнішній поверхні конструкцій суттєво зростає за рахунок роботи вібровипромінювачів. Результати віброприскорення контрольного розрахунку на зовнішній поверхні стіни при увімкненій САЗ наведені на рисунку 3.2.

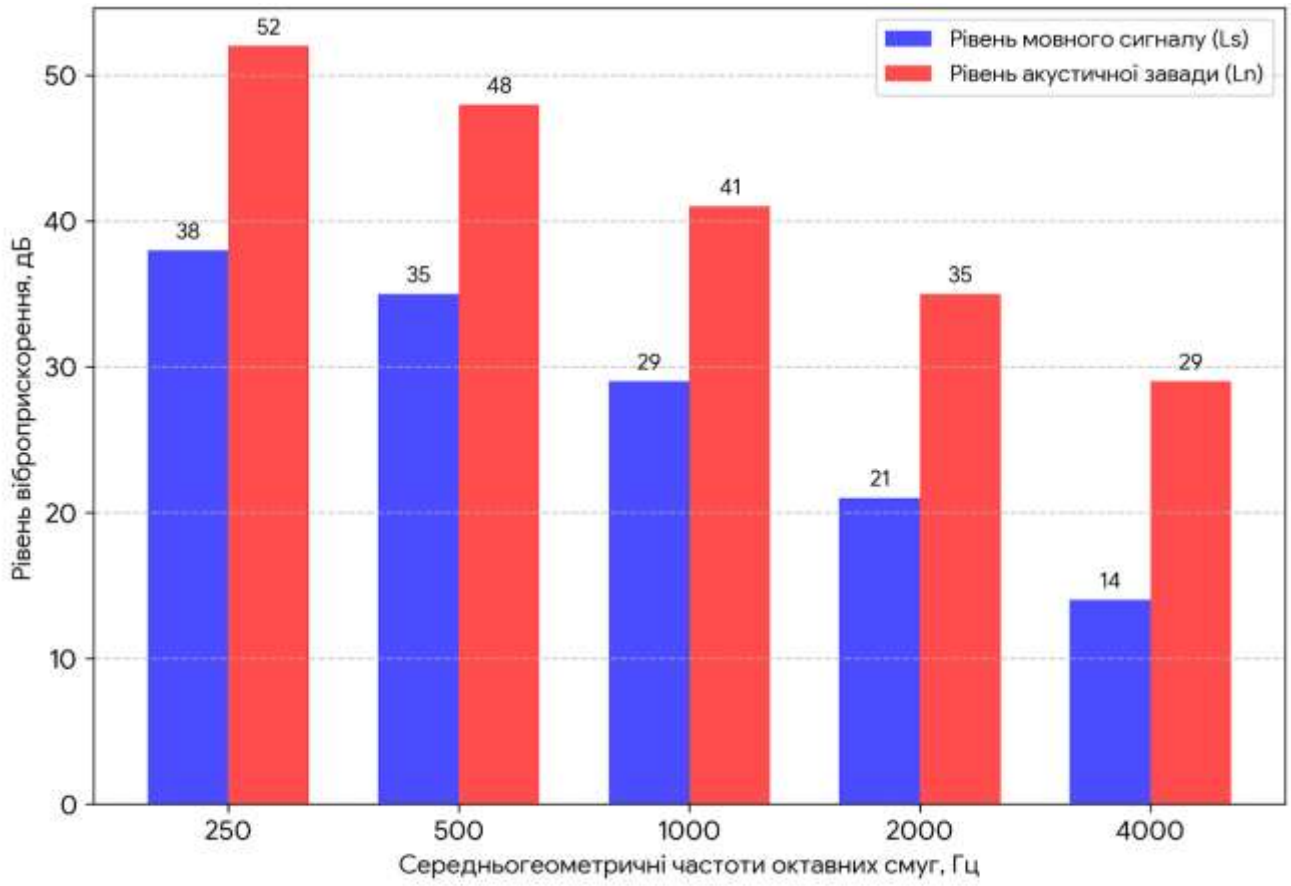

Рис. 3.2 Розподіл сигналу та завади на поверхні стіни при активному САЗ

Для порівняльного аналізу показників захищеності після впровадження системи запишемо дані в таблицю 3.2 та проведем обрахунки індексу артикуляції.

Таблиця 3.2

Вимірювання значень досліду стіни з САЗ

Частота, Гц	Рівень сигналу, L_s (дБ)	Рівень завади, L_n (дБ)	Відношення сигнал/шум, SNR (дБ)	Вагові коефіцієнти, W_i	Коефіцієнт сприйняття, L_i
250	38	52	-14	0.113	0.033
500	35	48	-13	0.205	0.067
1000	29	41	-12	0.207	0.1
2000	21	35	-14	0.275	0.033
4000	14	29	-15	0.200	0

Обрахунки коефіцієнтів сприйняття в яких значення SNR лежить у межах (-15дБ; +15дБ):

$$L_{i250} = \frac{(-14+15)}{30} = 0.033, \qquad L_{i500} = \frac{(-13+15)}{30} = 0.067,$$

$$L_{i1000} = \frac{(-12+15)}{30} = 0.1, \qquad L_{i2000} = \frac{(-14+15)}{30} = 0.033;$$

Розрахунок індексу R:

$$R = (0.113 * 0.033) + (0.205 * 0.067) + (0.207 * 0.1) + (0.275 * 0.033) = 0.0472 \approx 0.05$$

Після вмикання САЗ, за тих самих умов дослідження стіни, індекс артикуляції знизився до R = 0.05, що відповідає словесній розбірливості W ≈ 9 %.

На гістограмі розподілу (рис.3.3) для віконного скла наочно відображено результат роботи вібровипромінювачів, де інтенсивна завада повністю перекриває інформативний сигнал, усуваючи загрозу витоку.

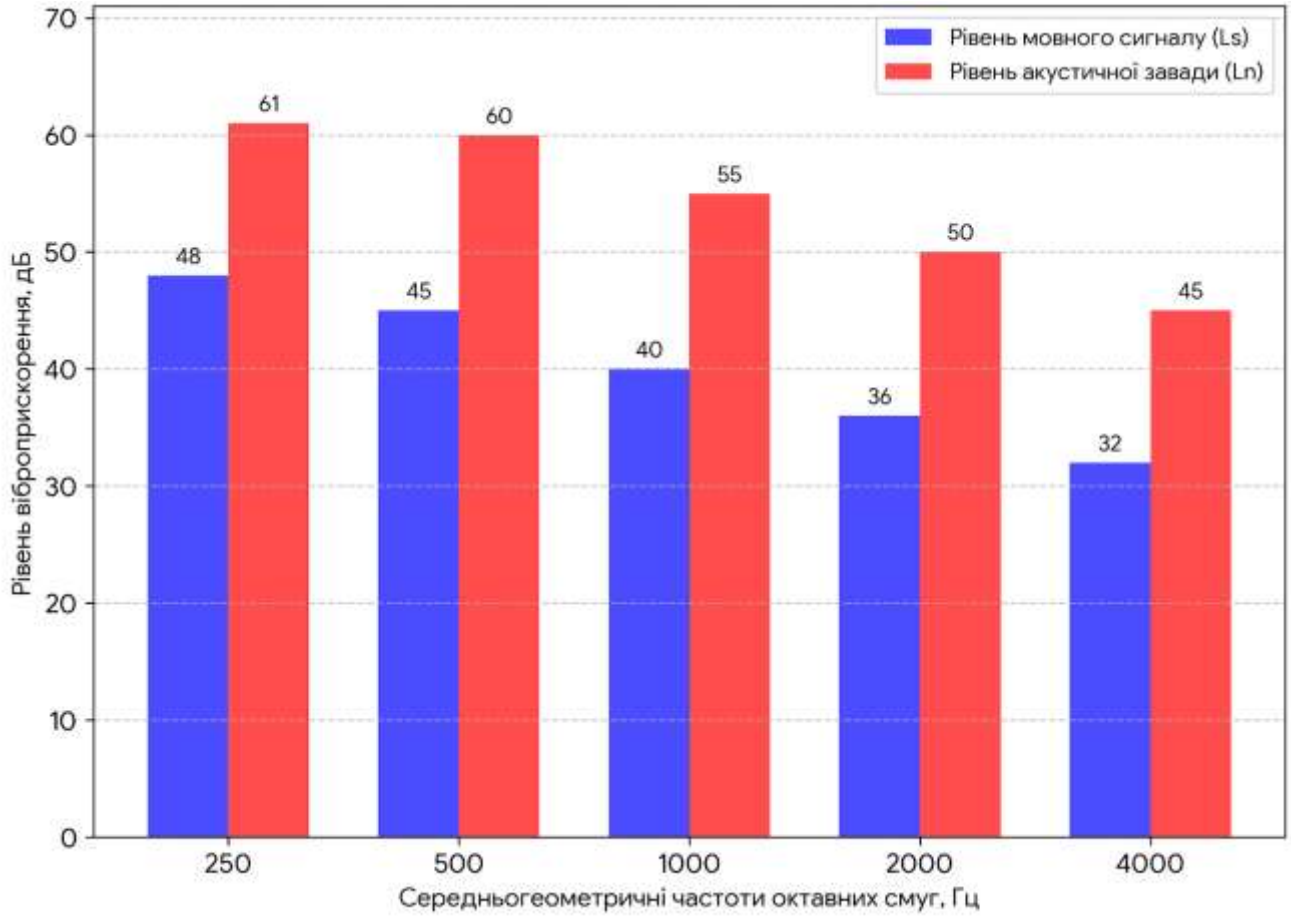

Рис. 3.3 Розподіл сигналу та завади на поверхні віконного скла при активному САЗ

Для визначення рівня захищеності об'єкта при функціонуванні САЗ виконано відповідні розрахунки для отримання інтегрального індексу артикуляції. Узагальнені результати вимірювань рівнів сигналу та шуму представлено в таблиці 3.3

Таблиця 3.3

Вимірювання значень досліду вікна з САЗ

Частота, Гц	Рівень сигналу, L_s (дБ)	Рівень завади, L_n (дБ)	Відношення сигнал/шум, SNR (дБ)	Вагові коефіцієнти, W_i	Коефіцієнт сприйняття, L_i
250	48	61	-13	0.113	0.067
500	45	60	-15	0.205	0
1000	40	55	-15	0.207	0
2000	36	50	-14	0.275	0.033
4000	32	45	-13	0.200	0.067

Обрахунки коефіцієнтів сприйняття в яких значення SNR лежить у межах (-15дБ; +15дБ):

$$L_{i250} = \frac{(-13+15)}{30} = 0.067, \quad L_{i2000} = \frac{(-14+15)}{30} = 0.033, \quad L_{i4000} = \frac{(-13+15)}{30} = 0.067;$$

Розрахунок індексу R:

$$R = (0.113 * 0.067) + (0.275 * 0.033) + (0.200 * 0.067) = 0.03$$

Після вмикання САЗ, за тих самих умов дослідження вікна, індекс артикуляції знизився до R = 0.03, що відповідає словесній розбірливості W ≈ 4 %.

Ефективність захисту інженерних комунікацій ілюструє наступний графік (рис. 3.4), де зафіксовано значне перевищення рівня завади над сигналом завдяки високій акустичній провідності металу труб.

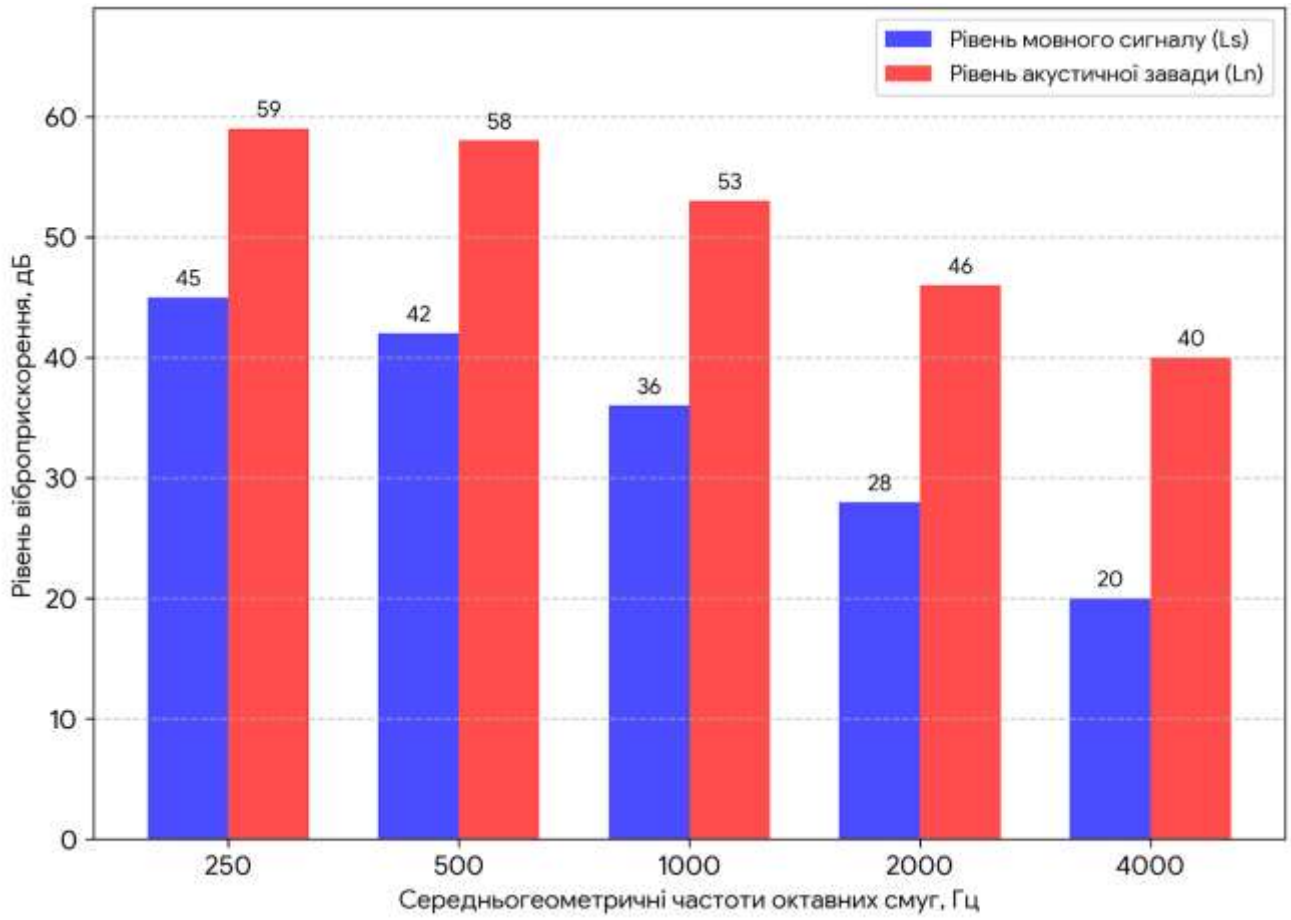

Рис. 3.4 Розподіл сигналу та завади на комунікаціях системи опалення при активному САЗ

Результати інструментального контролю ефективності системи активного зашумлення та розрахунок показників розбірливості мови для даного режиму роботи зведено в таблиці 3.4.

Таблиця 3.4

Вимірювання значень досліду радіатора з САЗ

Частота, Гц	Рівень сигналу, L_s (дБ)	Рівень завади, L_n (дБ)	Відношення сигнал/шум, SNR (дБ)	Вагові коефіцієнти, W_i	Коефіцієнт сприйняття, L_i
250	45	59	-14	0.113	0.033
500	42	58	-16	0.205	0
1000	36	53	-17	0.207	0
2000	28	46	-18	0.275	0
4000	20	40	-20	0.200	0

Обрахунки коефіцієнтів сприйняття в яких значення SNR лежить у межах (-15дБ; +15дБ):

$$L_{i250} = \frac{(-14 + 15)}{30} = 0.033;$$

Розрахунок індексу R:

$$R = (0.113 * 0.033) = 0.0037 \approx 0.004$$

Після вмикання САЗ, за тих самих умов дослідження систем опалення, індекс артикуляції знизився до R = 0.004, що відповідає словесній розбірливості W ≈ 0 %.

Як продемонстрували результати експериментальних досліджень, використання САЗ є високоефективним методом технічного захисту, що дозволяє критично зменшити витік інформації віброакустичним каналом. Незалежно від фізичних властивостей середовища поширення сигналу, генерація маскуючої завади забезпечила зниження словесної розбірливості з небезпечного рівня 97–100% до значень, що не перевищують 9%, гарантуючи виконання нормативних вимог захищеності.

3.2. Заходи щодо блокування каналів ПЕМВН

Було досліджено, що інтерфейсні кабелі відеосистеми, зокрема, стандарту HDMI та USB, виступають джерелом інтенсивного електромагнітного випромінювання, яке містить інформативні ознаки відеозображення. Високий рівень сигналу на тактових частотах створює передумови для безконтактного перехоплення інформації. Для нейтралізації цієї загрози пропонується застосування методу пасивного захисту, який полягає в локалізації електромагнітного поля в межах кабельної мережі за допомогою екранування та фільтрації.

Основним рекомендованим заходом є повна заміна стандартних з'єднувальних кабелів на спеціалізовані захищені версії. Технічні вимоги до нового кабелю передбачають використання багатошарової системи екранування. Конструкція такого кабелю повинна включати індивідуальне екранування кожної сигнальної пари алюмінієвою фольгою для запобігання перехресним завадам, а також загальне екрануюче обплетення з мідної сітки, що покриває весь пучок провідників. Таке рішення дозволяє створити замкнений контур навколо провідників, що перешкоджає виходу електромагнітної енергії у зовнішнє середовище.

Додатковим елементом пасивного захисту є використання феритових фільтрів на обох кінцях кабелю. Феромагнітний матеріал фільтра діє як індуктивний опір для високочастотних струмів, ефективно поглинаючи синфазні завади, що виникають на обплетенні кабелю, та перетворюючи їх на теплову енергію. Це запобігає перетворенню зовнішньої оболонки кабелю на передавальну антену.

Для підтвердження ефективності запропонованих заходів було проведено повторний інструментальний контроль після заміни стандартних кабелів на екрановані з феритовими фільтрами. Результати контрольного вимірювання наведені на спектрограмі (рис. 3.5-3.6).

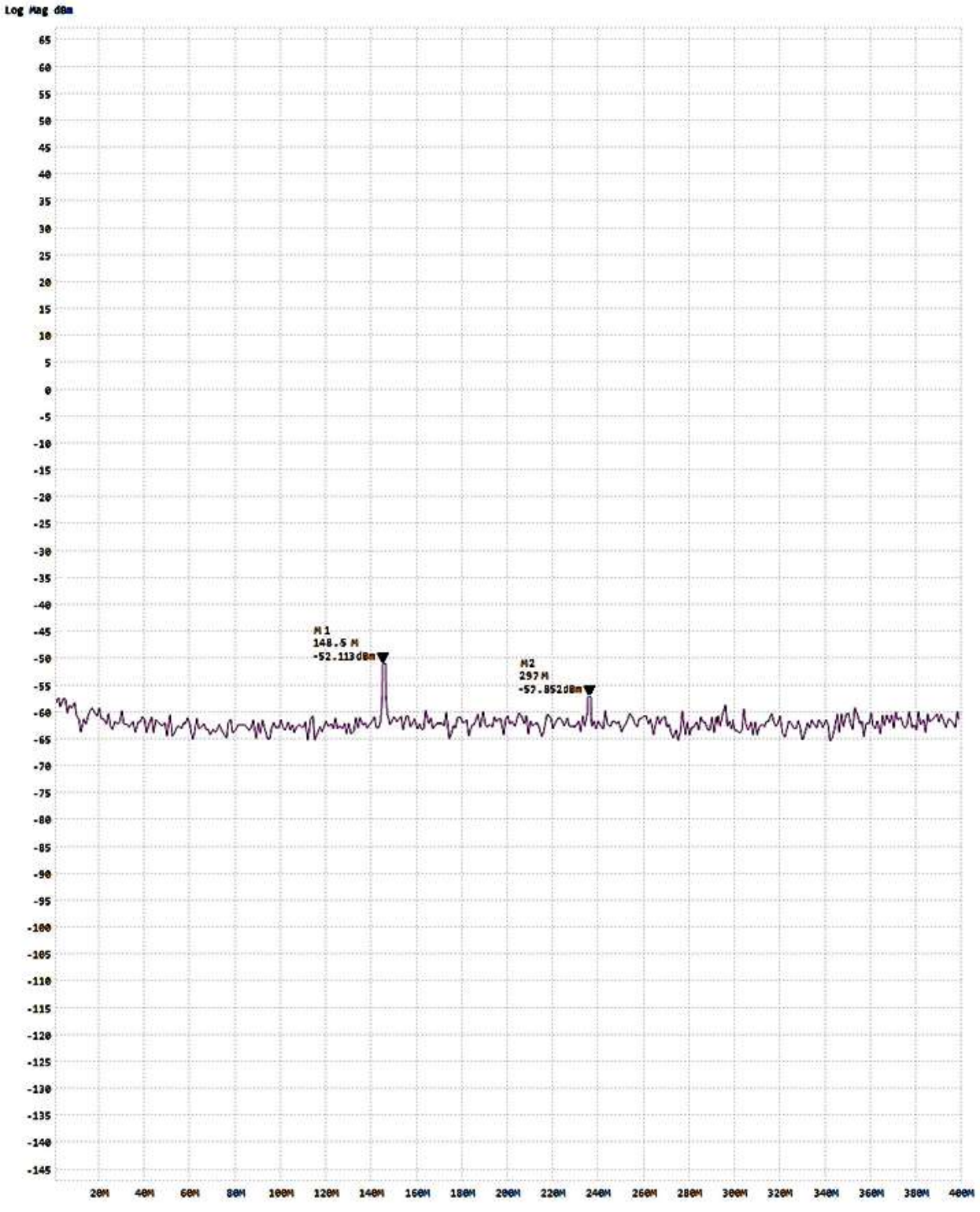

Рис. 3.5 Спектрограма випромінювання екранованого кабелю HDMI з феритовими фільтрами

Аналіз отриманої спектрограми демонструє кардинальне зниження рівня побічних випромінювань. Амплітуда основної гармоніки на частоті 148.5 МГц знизилася з початкових -7.7 dBm до рівня -52.1 dBm. Розрахунковий коефіцієнт екранування склав приблизно 44 дБ. В той час друга гармоніка на частоті 297 МГц

знизилася з -16.3 dBm до -57.9 dBm. Розрахунковий коефіцієнт екранування склав приблизно 41 дБ.

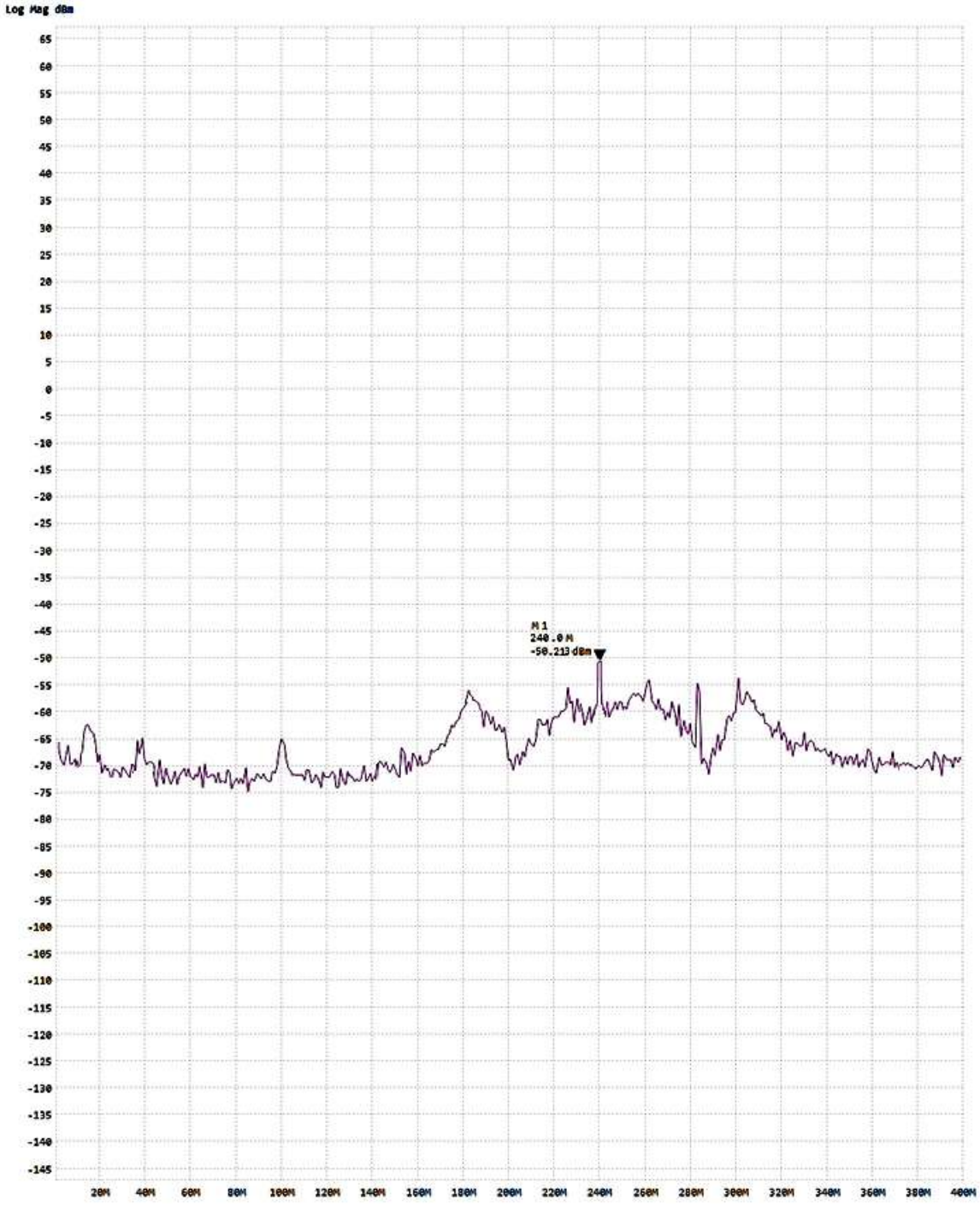

Рис. 3.6 Спектрограма випромінювання екранованого кабелю USB з феритовими фільтрами

Амплітуда даної спектограми на частоті 240 МГц знизилася з початкових -25 dBm до рівня -50 dBm. Розрахунковий коефіцієнт екранування склав приблизно 25 дБ.

Залишковий рівень сигналу у двох випадках лише незначно перевищує рівень власних шумів вимірювального приладу, що критично зменшує радіус можливого перехоплення з кількох метрів до 40 сантиметрів від поверхні кабелю. Таким чином, загроза витоку візуальної інформації електромагнітним каналом повністю нейтралізована без необхідності застосування активних генераторів шуму.

3.3. Технічний захист акустичного каналу

Після реалізації заходів віброакустичного захисту огороджувальних конструкцій залишається невирішеною проблема прямого поширення звукових хвиль через технологічні отвори, зокрема систему вентиляції та нещільності дверних блоків. Оскільки ці канали є повітряними хвилеводами, застосування вібраційних засобів PIAC для них є неефективним, тому розроблено окремий комплекс заходів блокування.

Особливу загрозу становить вентиляційний канал, який має прямий вихід за межі контрольованої зони на фасад будівлі. Для надійного перекриття цього каналу рекомендується застосування комбінованого методу захисту, що поєднує активні та пасивні засоби. Суть методу полягає в інтеграції безпосередньо у порожнину повітроводу акустичного випромінювача, підключеного до генератора рожевого шуму. У якості центрального блоку генерації пропонується використання системи акустичного захисту «Базальт-4 ГА»[14, 15]. Даний прилад є багатоканальним генератором, що дозволяє незалежно налаштовувати рівень маскуючого сигналу для акустичного каналу системи вентиляції. Технічні характеристики генератора дозволяють формувати білий, рожевий або мовленнєвоподібний шум у діапазоні частот від 100 Гц до 10 кГц, що повністю перекриває спектр мовного сигналу та забезпечує максимальний коефіцієнт маскування.

Безпосередньо для створення акустичної завади всередині повітроводу обрано випромінювач акустичний ВА-1. Це спеціалізований динамік, розроблений для встановлення всередину порожнин та технологічних каналів. Критично важливою особливістю його конструкції є вологозахищений корпус, що гарантує стабільну роботу в умовах можливого утворення конденсату у вентиляційній системі. Монтаж випромінювача здійснюється всередині короба на спеціальному

кронштейні у бік виходу повітря на фасад, що забезпечує необхідну спрямованість завади.

Вибір саме цих компонентів обумовлений їх повною електричною сумісністю. Запропонований випромінювач ВА-1 електрично узгоджений з вихідним каскадом генератора «Базальт-4 ГА», що дозволяє підключити його до окремого регульованого каналу. Це дає можливість виставити необхідний рівень звукового тиску всередині труби (наприклад, 75-80 дБ) незалежно від налаштувань вібровипромінювачів на вікнах. Така архітектура дозволяє створити єдину централізовану систему управління захистом, що значно спрощує експлуатацію комплексу.

Критичним аспектом експлуатації активних систем захисту акустичного каналу є дотримання балансу між захищеністю інформації та комфортними умовами праці, оскільки функціонування акустичного випромінювача не повинно створювати перешкод для розбірливості мови учасників наради всередині приміщення. Для мінімізації впливу шумової завади на персонал передбачено комплекс інженерних рішень.

По-перше, монтаж динаміка ВА-1 здійснюється з урахуванням фактору спрямованості, вектор поширення звукової хвилі орієнтується від приміщення назовні. Завдяки цьому основна енергія шуму концентрується у зоні можливого перехоплення, а у приміщення потрапляє лише значно ослаблений відбитий сигнал.

По-друге, застосовується метод психоакустичної адаптації спектра завади. Генератор налаштовується на формування рожевого шуму, спектральна щільність якого спадає з підвищенням частоти. На слух такий сигнал сприймається як монотонний фоновий шум руху повітря, аналогічний до роботи системи кондиціонування, і не викликає у персоналу подразнення чи втоми, на відміну від різкого білого шуму.

По-третє, здійснюється суворе нормування рівня гучності залишкового шуму в точці розміщення учасників наради. Налаштування системи виконується таким чином, щоб рівень шуму біля столу переговорів не перевищував 35-40 дБ. Враховуючи, що рівень гучності звичайної мови становить 60–65 дБ, відношення

сигнал/шум усередині приміщення залишається комфортним для спілкування (SNR>20 дБ), тоді як у вентиляційному каналі воно стає негативним, надійно блокуючи витік інформації.

Однак використання лише активного генератора призведе до демаскування системи захисту через вихід значного рівня шуму назовні. Тому другим обов'язковим компонентом системи є встановлення пасивного канального шумоглушника трубчастого або пластинчастого типу. Шумоглушник монтується на ділянці повітроводу між акустичним випромінювачем та вихідною решіткою. Його функція - поглинання енергії як залишкового мовного сигналу, так і генерованої шумової завади. Така конфігурація забезпечує повну акустичну непрозорість каналу при збереженні акустичного комфорту на прилеглій території.

Щодо захисту дверного отвору, основною проблемою є проходження звукових хвиль крізь мікрощілини у місцях прилягання дверного полотна до коробки та підлоги. Для блокування цього шляху витоку необхідна ретельна герметизація периметра дверей. Рекомендовано встановлення подвійного контуру гумових ущільнювачів по всьому периметру коробки, що забезпечує щільний притул та підвищує звукоізоляцію конструкції на 5-7 дБ.

3.4. Рекомендації щодо захисту дротових комунікацій та електроакустичних перетворювачів

Окрім прямого електромагнітного випромінювання від відеокабелів, суттєву загрозу становить наведення інформативних сигналів на струмопровідні лінії, що виходять за межі контрольованої зони. Найбільш вразливими є мережі передачі даних Ethernet та лінії підключення периферійного аудіообладнання. Для нейтралізації цих каналів пропонується комплекс заходів з модернізації кабельної інфраструктури та встановлення завадозахисних пристроїв.

Критичним етапом вдосконалення системи захисту є модернізація локальної обчислювальної мережі шляхом переходу на волоконно-оптичні лінії зв'язку. Стандартний мідний кабель типу кручена пара, що використовується для підключення до мережі Інтернет, здатен виконувати роль антени, приймаючи наведення від роботи технічних засобів обробки інформації та транслюючи їх у

загальну мережу будівлі. Для усунення цього каналу рекомендується повна відмова від використання провідників з металевою жилою на ділянці магістрального підключення виділеного приміщення. У приміщенні встановлюється медіаконвертер, що перетворює електричний сигнал на оптичний. Далі з’єднання з комутаційною шафою в коридорі відбувається через оптоволоконний кабель. Оскільки оптичне волокно є діелектриком, воно не проводить електричний струм, не створює власного електромагнітного поля та абсолютно нечутливе до зовнішніх наведень, що забезпечує повну розв’язку та гарантований захист від витоку інформації через мережевий кабель.

Другим напрямком захисту є блокування електроакустичного каналу витоку, пов'язаного з ефектом оборотності електроакустичних перетворювачів та можливостю високочастотного нав’язування. Динамічні голівки гучномовців системи оповіщення, а також мікрофони конференцсистеми, навіть у вимкненому стані можуть під дією акустичних хвиль генерувати слабкі електричні сигнали, що поширюються по з’єднувальних лініях за межі приміщення. Для протидії цьому явищу необхідно обладнати всі лінії, що перетинають межу контрольованої зони, спеціалізованими фільтрами захисту інформації. Ці пасивні пристрої є фільтрами низьких частот, які пропускають корисний сигнал, наприклад, сигнал пожежної тривоги, але ефективно подавляють слабкі наведені сигнали мовного діапазону та блокують проходження високочастотних сигналів ззовні.

Додатково для захисту мікрофонів та акустичних систем, що використовуються під час нарад, рекомендується застосування схеми фізичного розриву лінії. Реалізація цього заходу передбачає встановлення комутаційних розмикачів, які забезпечують гальванічне відключення мікрофонів та гучномовців від підсилювальної апаратури та зовнішніх ліній у періоди, коли вони не використовуються за прямим призначенням. Таке рішення унеможливлює використання легальних засобів звукопідсилення, як пасивних підслуховуючих пристроїв навіть у випадку компрометації основного обладнання.

3.5. Забезпечення періодичного контролю ефективності захисту

Побудова технічого захисту інформації не обмежується лише встановленням та налаштуванням технічних засобів, оскільки в процесі експлуатації можлива зміна параметрів обладнання, вихід з ладу окремих компонентів або поява нових загроз. Для гарантування стабільності показників захищеності необхідно впровадити процедуру періодичного інструментального контролю радіоелектронної обстановки в приміщенні. З огляду на високу вартість та складність експлуатації професійних вимірювальних комплексів для щоденного моніторингу, економічно та технічно обгрунтованим є використання сучасних портативних аналізаторів спектра інженерного класу, наприклад вже використовуваний tinySA Ultra.

Використання даного приладу дозволяє вирішувати декілька критично важливих задач технічного контролю без залучення сторонніх лабораторій. Першочерговою функцією є перевірка працездатності систем цілісності екранування. Оскільки система захисту від ПЕМВН базується на використанні екранованих кабелів, будь-яке механічне пошкодження екрана, окислення контактів або помилкова заміна кабелю на стандартний під час обслуговування техніки може призвести до відновлення каналу витоку. Оператор за допомогою аналізатора здійснює контрольні заміри біля інтерфейсних кабелів. Відсутність на спектрограмі характерних гармонік відеосигналу, які були зафіксовані під час первинного обстеження, є підтвердженням ефективності екранування.

Крім контролю власних засобів захисту, портативний аналізатор дозволяє проводити оперативний пошук несанкціонованих джерел випромінювання. Методика експрес-аналізу передбачає сканування радіоефіру перед початком важливих нарад. Наявність на спектрограмі локальних максимумів амплітуди, які не відповідають частотам використовуваних засобів зв'язку та відсутні у паспорті радіоелектронної обстановки приміщення, може свідчити про роботу прихованих підслуховуючих пристроїв, що передають інформацію радіоканалом. Впровадження регламенту обов’язкового передсеансового моніторингу за

допомогою портативних засобів дозволяє значно підвищити рівень оперативного захисту об’єкта інформаційної діяльності.

Висновки до третього розділу

У даному розділі розроблено та обгрунтовано рекомендації для впровадження комплексу технічних заходів, спрямованих на нейтралізацію виявлених каналів витоку інформації та створення надійної системи захисту ОІД.

Для перекриття віброакустичного каналу витоку запропоновано впровадження САЗ. Обґрунтовано вибір виконавчих елементів: п’єзоелектричних вібровипромінювачів РІАС-2ВП для віконних конструкцій та електромагнітних РІАС-2ГС для масивних стін і труб опалення. Розрахунковим шляхом доведено, що застосування даної системи дозволяє знизити коефіцієнт словесної розбірливості мови на зовнішніх поверхнях з критичних 97% до безпечного рівня 5–10%, що гарантує неможливість відновлення змісту переговорів.

Для блокування каналу ПЕМВН обрано стратегію пасивного захисту. Експериментально підтверджено, що заміна стандартних інтерфейсних кабелів відеосистеми на спеціалізовані екрановані кабелі з феритовими фільтрами забезпечує зниження рівня інформативних гармонік на 35-40 дБ. Це дозволяє локалізувати електромагнітне поле в межах кабельної мережі без застосування додаткових генераторів шуму.

Розроблено комбінований метод захисту акустичного каналу через систему вентиляції, що поєднує встановлення активного акустичного випромінювача всередині повітроводу та пасивного шумоглушника. Таке рішення забезпечує акустичну непрозорість каналу при збереженні комфортних умов для персоналу.

Для захисту від витоку через дротові комунікації та електроакустичні перетворювачі рекомендовано модернізацію локальної мережі з переходом на волоконно-оптичні лінії зв'язку, що виключає можливість наведення інформативних сигналів. Захист ліній мікрофонів та динаміків забезпечується встановленням завадозахисних фільтрів та пристроїв фізичного розриву кола.

Обґрунтовано необхідність та визначено методику періодичного інструментального контролю захищеності за допомогою портативних аналізаторів спектра. Це дозволяє оперативно виявляти порушення цілісності екранування, контролювати роботу систем активного захисту та виявляти несанкціоновані радіоелектронні пристрої.

ВИСНОВКИ

У даній дипломній роботі вирішено актуальне науково-прикладне завдання, що полягає у дослідженні шляхів та виробленні обгрунтованих рекомендацій щодо технічного захисту інформації на об’єкті інформаційної діяльності. На основі комплексного підходу, що поєднує теоретичний аналіз, моделювання досліджень та інструментальні вимірювання, отримано наступні результати.

Теоретико-методологічний аналіз предметної області дозволив визначити інформацію як стратегічний актив, що потребує захисту за трьома фундаментальними параметрами: конфіденційність, цілісність та доступність. Проведено систематизацію нормативно-правової бази України у сфері ТЗІ, в результаті чого встановлено пріоритетність вимог НД ТЗІ для захисту об'єктів критичної інфраструктури та державних установ. Це означає необхідність безумовного блокування виявлених технічних каналів витоку незалежно від імовірності їх реалізації зловмисником. Розроблено класифікацію загроз, яка виокремлює технічні канали витоку як найбільш небезпечні для фізичного середовища об’єкта.

Дослідження фізичної природи технічних каналів витоку дало змогу деталізувати механізми перетворення інформаційних сигналів. Встановлено, що сучасні цифрові інтерфейси, системи вентиляції та будівельні конструкції виступають ефективними середовищами поширення небезпечних сигналів. Визначено, що перехоплення інформації можливе не лише у зоні прямої видимості, а й за рахунок побічних електромагнітних випромінювань та віброакустичних перетворень, для виявлення яких необхідні спеціалізовані засоби технічної розвідки.

В ході експериментального дослідження конкретного об’єкта інформаційної діяльності- зали нарад площею 78 кв. м виявлено критичні вразливості системи захисту. Інструментальний контроль віброакустичного каналу показав, що огороджувальні конструкції - стіни 200 мм, та інженерні комунікації - труби опалення, не забезпечують необхідного загасання сигналу. Розрахунковий

коефіцієнт словесної розбірливості мови на зовнішніх поверхнях досягав 97%, що свідчить про повну незахищеність приміщення від прослуховування.

Спектральний аналіз електромагнітного каналу зафіксував наявність потужного випромінювання від інтерфейсних кабелів відеосистеми на частотах 148,5 МГц, 240 МГц та 297 МГц з перевищенням над рівнем шуму до 50 дБ, що створює реальну загрозу дистанційного відновлення відеозображення. Також ідентифіковано акустичний канал витоку через систему вентиляції, що має прямий вихід за межі контрольованої зони.

Розроблено та обгрунтовано технічний захист інформації, який базується на поєднанні активних та пасивних методів протидії. Для нейтралізації віброакустичного каналу запропоновано впровадження системи активного зашумлення з використанням вібровипромінювачів РІАС-2ВП для вікон та РІАС-2ГС для стін і труб. Розрахунково доведено, що це знижує розбірливість мови до безпечного рівня 15% та нижче. Для захисту від ПЕМВН обрано стратегію пасивного екранування. Заміна кабелів на екрановані з феритовими фільтрами забезпечила зниження рівня побічних випромінювань на 35–40 дБ, локалізувавши сигнал у межах корпусу кабелю. Для перекриття каналу вентиляції розроблено комбіноване рішення, що включає встановлення активного акустичного випромінювача всередині каналу та пасивного шумоглушника, що забезпечує акустичну непрозорість повітроводу. Запропоновано модернізацію локальної мережі шляхом переходу на волоконно-оптичні лінії зв’язку для усунення загрози наведень.

Сформовано організаційно-технічні рекомендації, що включають використання захисних ролетів та забезпечення періодичного інструментального контролю захищеності за допомогою портативних аналізаторів спектра. Результати роботи підтверджують, що запропонований комплекс заходів дозволяє створити систему захисту, яка перекриває всі виявлені канали витоку інформації. Реалізація наданих рекомендацій забезпечує приведення об’єкта інформаційної діяльності у

відповідність до вимог чинного законодавства України та гарантує збереження конфіденційності інформації під час проведення нарад і переговорів.

Оформлення результатів цього дослідження здійснювалося згідно з методичними рекомендаціями кафедри [24].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cyber Tactics: Lessons Learned in 2022. SSSCIP analytical report on the year of full-scale cyberwar against Ukraine. Kyiv : State Service of Special Communications and Information Protection of Ukraine, 2023. URL: https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine
2. Cost of a Data Breach Report 2023. IBM Security. 2023. P. 5–12. URL: https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf
3. Screen reading: Electromagnetic information leakage from the computer monitor / M. Grdović та ін. *Vojnotehnicki glasnik*. 2022. Т. 70, № 4. С. 836–855. URL: https://doi.org/10.5937/vojtehg70-38930
4. Романюк , В., & Платоненко, А. (2025). АНАЛІЗ ЯКОСТІ ГЕНЕРАТОРІВ РОЖЕВОГО ШУМУ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 789–799. URL: https://doi.org/10.28925/2663-4023.2025.29.940
5. Романюк В., Платоненко А. Дослідження ефективності системи акустичного зашумлення від витоку акустичної інформації. Студентська наукова конференція «Безпека інформаційно-комунікаційних систем», Київ: Київ. ун-т ім. Б. Грінченка, 2025. С.102–105. URL: https://fitm.kubg.edu.ua//konferentsii-fakultetu.html
6. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР-1994 - № 31. - Ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
7. Закон України «Про державну таємницю» URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

8. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
9. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. навчальний посібник «Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації», Київ, 2016. URL: https://ela.kpi.ua/server/api/core/bitstreams/930d9270-2cb1-4c62-a4ce-ab5404d9b90f/content
10. Барабаш, О., Аушева, Н., Складанний, П., Іваніченко, Є., & Довженко, Н. (2024). Технічні аспекти побудови відмовостійкої інфраструктури сенсорної мережі. Кібербезпека: освіта, наука, техніка, 4(24), 185–195. https://doi.org/10.28925/2663-4023.2024.24.185195
11. Василюк, В. Об’єкти захисту інформації. Методи та засоби захисту інформації / науково-технічний збірник. - Київ : НТУУ «КПІ» - 2006. - С. 88-95. URL: https://ela.kpi.ua/items/fdb6f84b-73f0-4db0-9549-c794e582ea21
12. Методика контролю захищеності мовної інформації від витоку акустичним та віброакустичним каналами [Текст]: НД ТЗІ 2.3-017-08. [Чинний від 2008-08-26]. – К. : Державна служба спеціального зв'язку та захисту інформації України, 2008. – 18 с. – (Нормативний документ системи технічного захисту інформації).
13. Прокофьєв М., Стеченко В. Дослідження витоку інформації каналами ПЕМВН у мережу електроживлення. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2(19) вип., 2009 р. URL: https://ela.kpi.ua/server/api/core/bitstreams/aeec4b31-ce07-4b0e-9281-6313145b410c/content
14. Захист інформації від витоку технічними каналами. URL: https://tzi.com.ua/zaxist-nformacz-vd-vitoku-texnchnimikanalami.html
15. Загальний огляд систем віброакустичного зашумлення. URL: https://tzi.com.ua/zagalnij-oglyad-sistem-vbroakustichnogo-zashumlennya.html
16. Астапеня В., Марценюк М., Шевченко С., Складанний П., Марценюк Є. (2021). Експериментальні дослідження впливу екранів і засобів захисту на

рівень акустичного сигналу у приміщенні із скляними та металопластиковими конструкціями. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 4(12), 117-131. https://doi.org/10.28925/2663-4023.2021.12.117131

17. Марценюк М., Складанний П., Астапеня В. (2021). Експериментальні дослідження стенду імітаційного моделювання роботи лазерного мікрофону для зняття акустичної інформації. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка;, 2(14), 131-147. https://doi.org/10.28925/2663-4023.2021.14.131147
18. Задворний, Д., Козачок, В., Черевик, В., Бодненко, Д., & Добришин, Ю. (2025). Методи та засоби побудови комплексної системи захисту інформації типового об’єкта інформаційної діяльності. Кібербезпека: освіта, наука, техніка, 3(31), 762–772. https://doi.org/10.28925/2663-4023.2025.31.1073
19. Соколов, В., Новицький, А., & Бодненко, Д. (2025). Імітаційне моделювання конфліктної взаємодії BLE-пакетів. Кібербезпека: освіта, наука, техніка, 2(30), 662–681. https://doi.org/10.28925/2663-4023.2025.30.997
20. V. Astapenya, et al., Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 290–300.
21. O. Mykhaylova, et al., Resistance to Replay Attacks of Remote Control Protocols using the 433 MHz Radio Channel, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 98–110.
22. Крючкова, Л., & Ворохоб, Н. (2025). Адаптивні методи протидії активним шумовим завадам. Кібербезпека: освіта, наука, техніка, 2(30), 455–472. https://doi.org/10.28925/2663-4023.2025.30.987
23. Крючкова, Л., & Шандрук, М. (2025). Методи протидії в радіонавігаційних конфліктах. Кібербезпека: освіта, наука, техніка, 4(28), 766–780. https://doi.org/10.28925/2663-4023.2025.28.863
24. Жданова, Ю. Д., Складанний, П. М., & Шевченко, С. М. (2023). Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для

студентів спеціальності 125 Кібербезпека та захист інформації. https://elibrary.kubg.edu.ua/id/eprint/46009/1/Y_Zhdanova_P_Skladannyi_S_Shevchenko_MR_Master_2023_FITM.pdf