

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування інституту, факультету)

Кафедра радіотехніки та телекомунікацій
(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

магістра

(ступінь вищої освіти)

на тему **ДИСТАНЦІЙНА СИСТЕМА КЕРУВАННЯ АКУСТИЧНИМ**
ЗАХИСТОМ КОНФЕРЕНЦЗАЛУ

Виконав(ла): студент(ка) 2м курсу, групи БК-912м

Спеціальності _____

172 «Телекомунікації та радіотехніка»

(код і найменування спеціальності)

Освітня програма (спеціалізація) _____

«Інформаційні мережі зв'язку»

ФЕДОРОВСЬКИЙ Дмитро Олександрович

(ПРИЗВИЩЕ та ініціали)

Керівник КОСТЕНКО Валер'ян Остапович

(ПРИЗВИЩЕ та ініціали)

Рецензент КАСЬЯН Микола Миколайович

(ПРИЗВИЩЕ та ініціали)

2023 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
 (повне найменування закладу вищої освіти)

Факультет Інформаційної безпеки та електронних комунікацій

Кафедра Радіотехніки та телекомунікацій

Ступінь вищої освіти магістр

Спеціальність 172 «Телекомунікації та радіотехніка»

(код і найменування)

Освітня програма (спеціалізація) Інформаційні мережі зв'язку

(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри РТТ

к.ф.-м.н., доц. Сергій САМОЙЛИК

« » грудня 2023 року

Сф

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

ФЕДОРОВСЬКОМУ Дмитру Олександровичу

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дистанційна система керування акустичним захистом конференцзалу

керівник проєкту (роботи) к.т.н., доцент, КОСТЕНКО Валер'ян Остапович

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

затверджені наказом закладу вищої освіти від «14» листопада 2023 року № 443

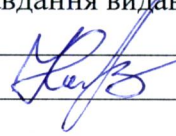
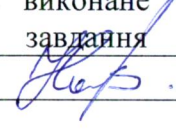
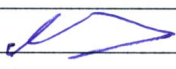
2. Строк подання студентом проєкту (роботи) 15 грудня 2023 року

3. Вихідні дані до проєкту (роботи) Знайти технічні засоби для дистанційної системи управління акустичним захистом конференцзалу та встановлення активних технологій захисту

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Знайти універсальний варіант дистанційного керування системою захисту, а також забезпечити живучість системи і її моніторинг

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів) презентація роботи в PowerPoint

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	КОСТЕНКОВ.О., доцент каф. РТТ		
Нормоконтроль	МОРОЗ Г.В., ст. викладач каф. РТТ		

7. Дата видачі завдання «17» жовтня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Огляд літератури та постановка задачі	2 тижні	виконано
2	Виявлення каналів витоку звуку під час діалогу	1 тиждень	виконано
3	Вивчення генераторів шуму та подавлювачів	1 тиждень	виконано
4	Створення записів про вибір та встановлення активних технологій для акустичного захисту	2 тижні	виконано
5	Вдосконалення системи та її живучості	3 тиждні	виконано
6	Оформлення ПЗ і презентації	1 тиждень	виконано
7	Захист роботи	1 день	виконано

Студент(ка)

(підпис)

(Ім'я ПРИЗВИЩЕ)



Дмитро ФЕДОРОВСЬКИЙ

Керівник проєкту (роботи)

(підпис)

(Ім'я ПРИЗВИЩЕ)



Валер'ян КОСТЕНКО

РЕФЕРАТ

Пояснювальна записка до магістерської роботи: 59 с., 2 табл., 29 рис., 17 джерел.

ВИТІК ІНФОРМАЦІЇ, АКУСТИЧНИЙ КАНАЛ, ГЕНЕРАТОРИ АКУСТИЧНИХ ПЕРЕШКОД, ЗВУКОІЗОЛЯЦІЯ, ПРОВАЙДЕР, РОУТЕР, ДЖЕРЕЛО БЕЗПЕРЕБІЙНОГО ЖИВЛЕННЯ, РЕЛЕ.

Найвищу цінність становить інформація, що передається усно. Усно повідомляють відомості, які можуть бути довірені технічним засобам передачі. Інформація, що оголошується під час переговорів, може містити конфіденційні або секретні відомості. Тому витік мовної інформації може становити серйозну загрозу економічній безпеці підприємства.

У цій роботі проведено аналіз можливих загроз безпеці мовної інформації, існуючих методів захисту. Розглянуто засоби активного захисту мовної інформації та застосовувані в них перешкоди. Для заданого плану приміщення запропоновано способи та матеріали звукоізоляції, а також технічні засоби постановки перешкод. Знайдено універсальний варіант дистанційного керування системою, а також забезпечено живучість системи і її моніторинг.

ЗМІСТ

	С.
Скорочення та умовні позначки	6
Вступ	7
1 Опис акустичного каналу витоку інформації	8
1.1 Підслуховування.....	9
1.2 Технічні канали витоку акустичної інформації	11
2 Розробка системи захисту	25
2.1 Пасивні методи захисту	25
2.2 Активні засоби захисту приміщень	33
2.3 Організаційні заходи під час проведення нарад	34
3 Розробка структурної схеми управління захистом.....	36
4 Вибір обладнання.....	40
4.1 Вибір провайдера.....	40
4.2 Вибір медіаконвертору.....	42
4.3 Вибір роутеру	44
4.4 Комплект відеоспостереження	46
4.5 Вибір реле	49
4.6 Вибір активних акустичних завад	51
4.7 Вибір ДБЖ	54
Висновки.....	56
Перелік джерел посилань.....	57

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

POE	—	Universal Serial Bus
USB	—	Universal Serial Bus
Wi-Fi	—	Wireless Fidelity
ВЧ	—	високі частоти
ДБЖ, UPS	—	джерело безперебійного живлення
ЕОМ	—	електронно-обчислювальна машина
СБ	—	служба безпеки
СБУ	—	служба безпеки України
ТСП	—	технічними засобами передачі інформації
ХС	—	характеристика спрямованості

ВСТУП

Несумнівно, інформація, що передається усно, має величезну цінність. Це особливо актуально, оскільки усно повідомлені відомості можна вважати надійними, і сучасні технології дозволяють визначити особистість говорячої особи. Отримана у момент висловлення інформація є найоперативнішою, що робить її особливо цінною для різноманітних сфер.

Ці характеристики викликають живий інтерес сторін, які конфліктують, до можливості прямого прослуховування мови, що коливається в приміщеннях через віброакустичні та акустичні канали. Тому питання захисту мовної інформації визнається пріоритетним при вирішенні завдань, пов'язаних із захистом від витоку даних через технічні канали.

Головною причиною промислового (економічного) шпигунства є прагнення до реалізації конкурентної переваги – найважливішої умови досягнення успіху в умовах ринкової економіки. Інформація, здобута таким шляхом, дозволяє бути в курсі справ конкурентів, використовувати їх науково-технічні досягнення, на основі чого можливе прийняття найбільш раціональних управлінських рішень, економія власних коштів на проведення НІОКР та фундаментальних досліджень. Економічне шпигунство може проводитися з метою отримання конфіденційної інформації для своєї вигоди. Цю інформацію використовують для власних стратегій, таких як оволодіння ринками, копіювання товарів конкурентів, дискредитація або пригнічення конкурентів, а також вплив на переговори та шантаж. оволодіння ринками збуту, підробки товарів, дискредитації або економічного придушення конкурентів, зриву переговорів щодо укладання контрактів, шантажу окремих осіб та ін.

1 ОПИС АКУСТИЧНОГО КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ

Канал витоку конфіденційної інформації – це фізичний шлях, що використовується для незаконного доступу до обмежених відомостей, і включає в себе використання енергетичних, просторових та часових параметрів, а також спеціальних технічних засобів для перехоплення і фіксації інформації.

Під час наради інформаційна безпека може бути піддана ризику через такі методи, як:

- підслуховування та запис мовної інформації через використання заставних пристроїв, стетоскопів, диктофонів та систем лазерного підслуховування;
- реєстрація сигналів учасників на неконтрольованій території через використання радіомікрофонів для виконання агентурних завдань;
- перехоплення електромагнітних випромінювань через звукозаписні пристрої та електроприлади;
- витік інформації через різні просторові елементи, такі як двері, вікна, стіни, підлога, стеля, а також через системи опалення та вентиляції.

Джерелами інформативно небезпечних сигналів у вигляді радіохвиль або електричних сигналів можуть бути звукопідсилювальні та звукозаписні засоби, сповіщувачі охоронної сигналізації, різні побутові прилади, розміщені в кімнаті для нарад. Відомий т.зв. мікрофонний ефект, тобто. модуляція параметрів радіоелементів під дією акустичних хвиль, що у свою чергу призводить до появи радіосигналів з інформативно небезпечною огиноючою. Так, наприклад, може бути модуляція параметрів елементівгетеродина побутового радіоприймача. Уразі відсутності розв'язки між антеною та гетеродином модульований сигнал гетеродина може бути прийнятий за межами приміщення.

Наявність спеціалістів із зовнішньої організації підвищує ризик створення додаткових шляхів витоку інформації. Це означає, що потенційний злоумисник може найняти когось із присутніх на нараді, отримуючи таким чином доступ до конфіденційної інформації.

Оскільки більшість інформації на нараді передається у формі мовної інформації, важливо враховувати, що мова представляє собою механічні коливання повітря, які, потрапляючи на тверді поверхні приміщення, перетворюються на вібраційні сигнали. Ці вібрації, залишаючись механічними, можуть поширюватися через будівельні конструкції на великі відстані.

В акустичному каналі можна виділити такі шляхи поширення акустичної хвилі:

- повітряне середовище кімнати;
- несучі стіни;
- тонкі стіни між кімнатою для проведення наради та кабінетами;
- двері;
- вентиляційний повітропровід.

Структурний звук також може використовувати різні механічні шляхи для передачі, включаючи стіни, перегородки, віконні рами, дверні коробки, трубопроводи та коробки вентиляції. Це вібрації можуть передаватися через тверді матеріали, дозволяючи злоумиснику отримувати інформацію через структурні компоненти будівлі.

1.1 Підслуховування

Загрозу безпеки мовної інформації може бути підслуховування: безпосереднє і підслуховування за допомогою технічних засобів.

Дані варіанти можна поділити на:

- а) підслуховування безпосередньо злоумисником:
 - підслуховування та запам'ятовування;

- підслуховування та запис;

б) підслуховування за допомогою технічних засобів:

- підслуховування шляхом прийому структурного звуку, що розповсюджується в трубах опалення та конструкціях будівлі;
- підслуховування за допомогою акустичних заставних пристроїв;
- перехоплення небезпечних сигналів технічних засобів;
- підслуховування з допомогою лазерних систем.

В процесі безпосереднього підслуховування акустичні сигнали, що поширюються у приміщенні, можуть бути сприйняті органами слуху зловмисника. Під час проведення наради можливі наступні варіанти підслуховування:

- через стіни та перегородки;
- через двері;
- через вікно (якщо воно нещільно закрите);
- через вентиляційний отвір.

У випадку, коли зловмисник є учасником наради, виявлення його дій може бути вкрай складним завданням, особливо якщо він не використовує спеціальні технічні засоби. Перевірка кандидатури кожного учасника на предмет його надійності та врахування особистих якостей стають ключовими аспектами забезпечення безпеки інформації під час наради. Професійна оцінка та ретельний відбір учасників є важливим етапом у зменшенні ризику витоку інформації.

У випадку безпосереднього підслуховування зловмисник може також вести реєстрацію підслуховуваної інформації, наприклад, шляхом запису на паперовий носій. Це вимагає ретельного контролю за навколишнім середовищем та може бути розкрито в разі виявлення підозрілого запису або дій учасника наради.

Щодо підслуховування через входні двері, це може бути складним завданням через наявність співробітників та служби безпеки в коридорі під

час робочого часу. Такі дії можуть привернути увагу і викликати підозри, що може призвести до швидкого виявлення зловмисника.

1.2 Технічні канали витоку акустичної інформації

1.2.1 Повітряні канали витоку

В повітряних каналах витоку інформації використовується повітря як середовище для поширення акустичних сигналів. Для захоплення цих сигналів використовуються невеликі та високочутливі мікрофони, а також спеціальні направлені мікрофони.

Основними джерелами акустичних коливань є механічні системи, такі як органи мови людини, та вторинні – різні перетворювачі, включаючи електроакустичні пристрої, наприклад, п'єзоелементи, мікрофони, телефони та гучномовці. Мовний сигнал, який є складним акустичним сигналом, покриває діапазон частот від 200...300 Гц до 4...6 кГц.

З метою збільшення дальності підслуховування широко використовуються заставні пристрої, розміщені у приміщенні зловмисниками або співробітниками, які маскують свою діяльність. Ці заставні пристрої можуть становити серйозну загрозу для безпеки конфіденційної інформації в обмежених зонах.

Мікрофони перетворюють акустичний сигнал на електричний, який потім може бути переданий на модулятор для перенесення інформації на високочастотне несуче коливання. Застосування антени для випромінювання радіосигналу дозволяє здійснювати передачу інформації в ефір.

Мініатюрні мікрофони можуть бути поєднані з різними пристроями, такими як портативні записуючі пристрої чи передавачі, а для ефективної передачі інформації використовуються різні види антен.

Загальна схема заставних пристроїв включає реєстраційні пристрої, які можуть бути розташовані у віддалених місцях, та можливості приховати передачу інформації від неповідомленого спостерігача.

Один із варіантів класифікації акустичних заставних пристроїв зображено на рисунку 1.1.



Рисунок 1.1 – Класифікація акустичних заставних пристроїв

Заставні пристрої, які використовуються для перехоплення інформації, переданої по повітрю, зазвичай використовують спеціальні приймальні пристрої, які функціонують у відповідному діапазоні довжин хвиль. Однак існують також заставні пристрої, які можуть бути встановлені безпосередньо в телефонні апарати. Ці пристрої можуть бути вбудовані в корпус телефону, відомий як "телефон-спостерігач", або підключені до телефонної лінії через телефонну розетку.

Такий пристрій, конструктивно об'єднуючи мініатюрний мікрофон і спеціальний блок комутації, часто отримує назву "телефонне вухо". Блок комутації дозволяє підключати мікрофон до телефонної лінії у визначених

умовах, таких як додзвін до "телефону-спостерігача" або надсилання спеціального кодованого сигналу по лінії.

Захоплення інформації відбувається, використовуючи мініатюрні мікрофони, які можуть бути поєднані з різними пристроями для запису або передачі отриманої інформації. При цьому існує можливість прослуховування розмов з іншого звичайного телефону, що дозволяє віддалено отримувати аудіосигнал.

Спрямовані мікрофони використовуються для прослуховування відкритих приміщень через відкриті вікна, двері або інші доступні отвори. Також може бути застосовано спеціальні види спрямованих мікрофонів, такі як параболічні, трубчасті (інтерференційні) та плоскі мікрофонні ґрати, для прослуховування розмов з відстані чи з інших будівель чи автомашин.

Параболічний мікрофон. Такий мікрофон має параболічний відбивач, у фокусі якого розміщується мікрофонний капсоль з ненаправленою або односпрямованою характеристикою спрямованості (ХН). Такі мікрофони іноді називають рефлекторними. Принцип дії рефлекторного мікрофона наведено на рисунку 1.2.

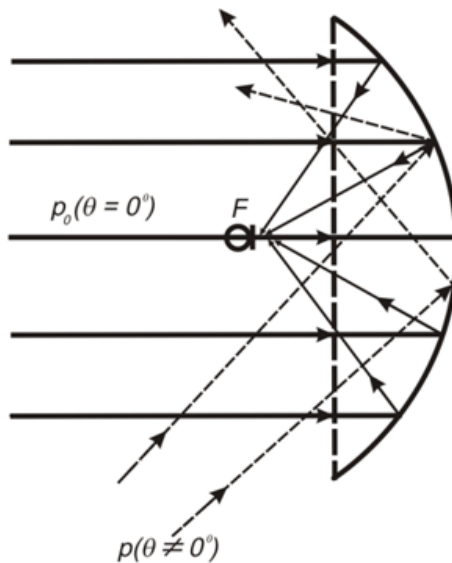


Рисунок 1.2 – Принцип дії параболічного мікрофона

Звукові хвилі, що прийшли з осьового напрямку параболи, відбиваються від відбивача і завдяки властивостям параболи після відбиття концентруються у фазі в її фокусі, де розташований мікрофонний капсуль. Звукові хвилі, що під кутом до осі параболи, розсіюються рефлектором, не потрапляючи на мікрофон. У рефлекторній системі ХН залежить від частоти і змінюється від практично ненаправленої на низьких частотах (при діаметрі рефлектора менше довжини звукової хвилі) до вузької пелюстки на високих частотах. Частотна характеристика чутливості таких мікрофонів має підйом у бік високих частот із крутістю близько 6 дБ на октаву, який зазвичай компенсується або електронним методом (наприклад, еквалайзером), або спеціальною конструкцією капсуля.

Мікрофон «біжучої хвилі» (інтерференційний). Подібні пристрої, які часто називають трубчастими мікрофонами, складаються з трубки з отворами або прорізами, на задньому торці якої розташований ненаправлений або односпрямований мікрофонний капсуль (рис. 1.3).

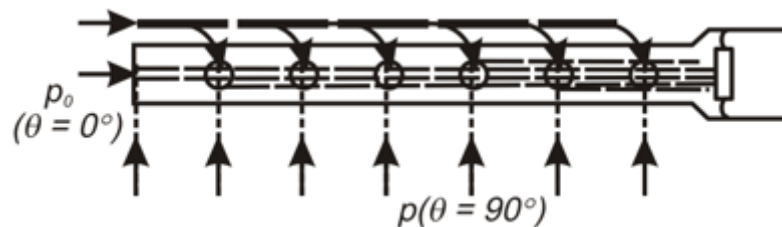


Рисунок 1.3 – Односпрямований мікрофонний капсуль

Отвори (прорізи) у трубці закриті тканиною або пористим матеріалом, акустичне опір якого зростає в міру наближення до капсуля. Звуження ХН досягається за рахунок інтерференції парціальних звукових хвиль, що проходять через отвори трубки. При русі фронту звукової хвилі паралельно осі трубки всі парціальні хвилі приходять до рухомого елемента одночасно, у фазі. При поширенні звуку під кутом до осі ці хвилі доходять до капсуля з

різною затримкою, що визначається відстанню від відповідного отвору до капсуля, при цьому відбувається часткова або повна компенсація тиску, що діє на рухомий елемент. Помітне звуження ХН у таких мікрофонах починається з частоти, де довжина трубки більше половини довжини звукової хвилі. Зі збільшенням частоти ХН ще більше звужується. Тому навіть при значній довжині таких мікрофонів, яка може досягати метра і більше, ХН на частотах нижче 150-200 Гц визначається лише капсулем і зазвичай близька до кардіоїди чи суперкардіоїди.

Трубчасті спрямовані мікрофони, порівняно з параболічними, більш компактні і використовуються в основному у випадках, коли необхідно забезпечити скритність прослуховування розмов. З використанням таких мікрофонів розвідку можна вести як з автомобіля, так і з вікна, розташованого навпроти будівлі.

Резонансний мікрофон. Резонансний мікрофон використовує принцип резонансу в металевих трубках різної довжини. Наприклад, в одній з його модифікацій мікрофон складається з набору з 37 трубок, довжина яких варіюється від 1 до 92 см. Звукові хвилі, які йдуть по осі трубок, надходять до приймача в однаковій фазі, тоді як ті, які приходять з бокових напрямків (завдяки різній довжині трубок та відмінності у швидкості поширення звукових хвиль у металі), виявляються зрушеними по фазі.

З точки зору скритності застосування спрямованих мікрофонів утруднене через часто неприйнятні їх габарити і джерела акустичних перешкод. Крім того, щоб не бути прослуханим в автомобілі, досить просто підняти скло. Нижче наведено малюнок направленого мікрофона резонансного (органного) типу (рис. 1.4).



Рисунок 1.4 – Зовнішній вигляд резонансного мікрофону

1.2.2 Вібраційний канал

В вібраційних або структурних каналах витоку інформації, акустичні сигнали поширюються через будівельні конструкції, такі як стіни, стелі, підлоги, а також трубопроводи водопостачання, опалення, каналізації та інші тверді об'єкти. Для перехоплення цих акустичних коливань застосовують контактні мікрофони, відомі як стетоскопи. Електронні стетоскопи, які з'єднані з електронним підсилювачем, можуть використовуватися для цієї мети.

Також можливе використання вібраційного каналу для передачі інформації за допомогою заставних пристроїв. Зазвичай ці пристрої використовують радіоканал для передачі інформації і, відповідно, їх називають радіостетоскопами. Також можливе використання заставних пристроїв для передачі інформації за допомогою оптичного каналу в

ближньому інфрачервоному діапазоні або за допомогою ультразвукового каналу, який може пройти через металеві конструкції будівлі.

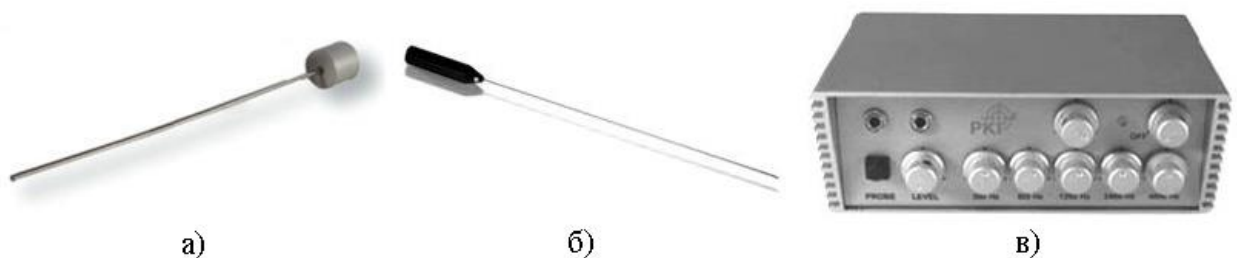
Гольчасті мікрофони та електронні стетоскопи.

Якщо є можливість доступу в суміжні з виділеним приміщенням, для прослуховування розмов можуть використовуватися голкові мікрофони (spike microphone) та електронні стетоскопи.

Виносні голчасті мікрофони є мікрофонами зі спеціальними тонкими звуководами і призначені для прослуховування розмов у суміжних приміщеннях через природні або спеціально створені щілини в конструкціях, що захищають контрольованих приміщень.

Наприклад, у системі PKI 2455 (рис. 1.5) використовується електретний голковий мікрофон з діаметром звуководу 2,5 мм та довжиною до 300 мм. Дальність перехоплення розмови до 10 м. Діаметр кабелю 2,5 мм. Підсилювач системи має масу 200г та розміри 95х60х25 мм. Живлення підсилювача здійснюється від акумулятора напругою 9 В. Час роботи від акумулятора до 60 год.

В електронних стетоскопах як датчики використовуються контактні мікрофони, які перетворюють акустичні коливання, що поширюються в твердих тілах (стінах, стелях), в електричні.



а – мікрофон PKI 2455; б – мікрофон XP-SP; в – підсилювач.

Рисунок 1.5 – система PKI 2455 з голчастими мікрофонами.

Електронні стетоскопи з контактними датчиками дозволяють перехоплювати мовну інформацію без необхідності фізичного доступу до виділених приміщень. Датчики таких стетоскопів часто розміщуються на зовнішніх поверхнях будівель, в оконних отворах та на віконних рамах. Також їх можуть встановлювати у суміжних, тобто службових та технічних приміщеннях, за дверними отворами, на конструкціях, що оточують, на перегородках, а також на трубах систем опалення та водопостачання, в коробах вентиляційних повітроводів та інших системах. Це дозволяє зломисникам отримувати конфіденційну інформацію, яка передається за допомогою акустичних сигналів, знаходячись поза приміщенням і без фізичного доступу до нього.

1.2.3 Електроакустичні канали витоку інформації

Електроакустичні технічні канали витоку інформації виникають шляхом здійснення електроакустичних перетворень, де акустичні сигнали перетворюються на електричні. Цей процес включає перехоплення акустичних коливань через ДТЗС, які виявляють "мікрофонний ефект", а також шляхом "високочастотного нав'язування" (рис. 1.6). Деякі елементи ДТЗС, такі як трансформатори, котушки індуктивності, електромагніти вторинних електрогодин, дзвінки телефонів, дроселі ламп та інші, можуть змінювати свої параметри під впливом акустичного поля, що веде до виникнення електричної реакції або модуляції струмів, передаючи інформаційний сигнал.

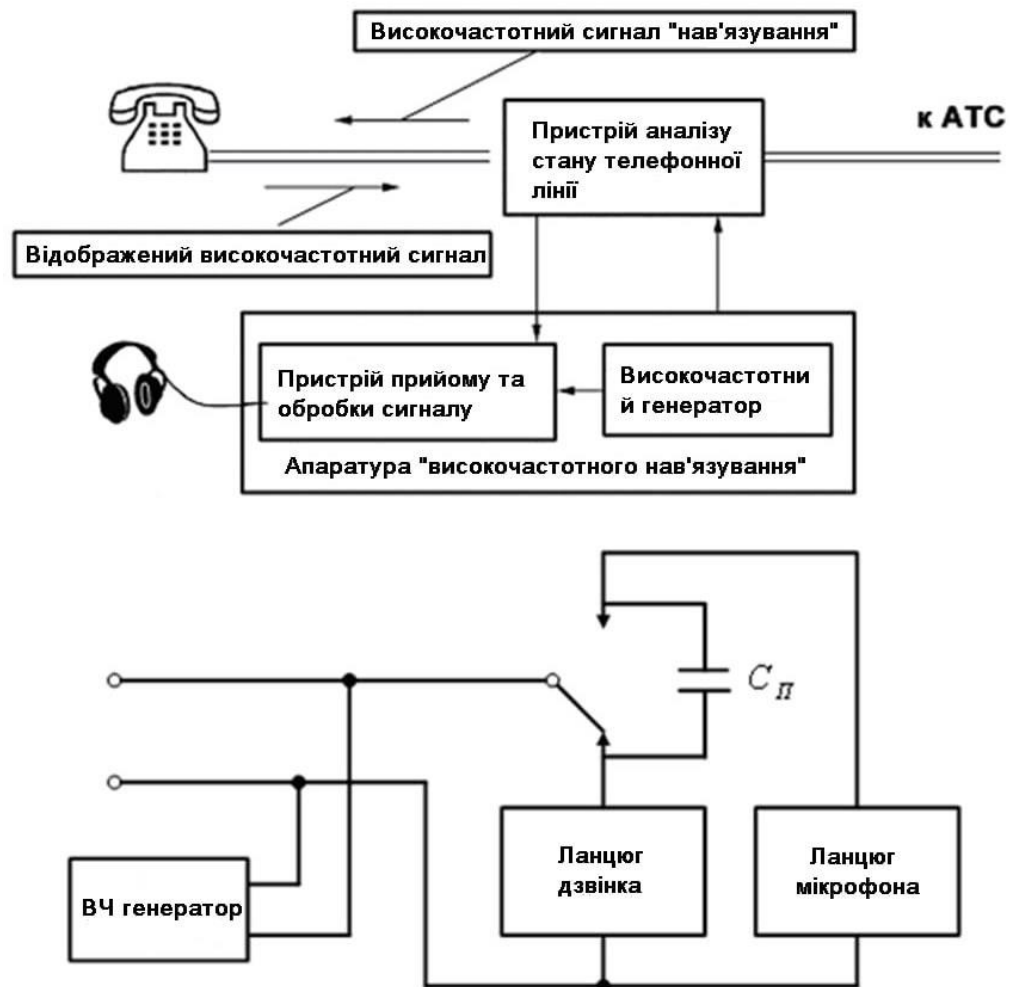


Рисунок 1.6 – Схема високочастотного навіязування

В електроакустичних технічних каналах витоку інформації використовуються джерела, такі як датчики пожежної сигналізації, динаміки ретрансляційної мережі тощо. Ефект електроакустичного перетворення акустичних коливань на електричні часто називається "мікрофонним ефектом". Деякі ДТЗС, які обладнані цим ефектом, найбільш чутливі до акустичного поля, зокрема абонентські гучномовці та деякі датчики пожежної сигналізації.

В цьому каналі витоку інформації акустичні коливання перехоплюються за допомогою підключення до з'єднувальних ліній ДТЗС, які обладнані "мікрофонним ефектом", за допомогою високочутливих низькочастотних підсилювачів. Наприклад, підключаючи такі засоби до

з'єднувальних ліній телефонів із електромеханічними викликами, можна прослуховувати розмови в приміщеннях, де встановлені ці апарати.

Технічний канал витоку інформації за допомогою "високочастотного наві'язування" може бути реалізований через несанкціоноване введення струмів високої частоти від відповідного генератора лінії, що має функціональні зв'язки з нелінійними або параметричними елементами ДТЗС. Ці елементи можуть модулювати високочастотний сигнал інформаційним сигналом. Високочастотний сигнал може відбиватися або випромінюватися, а для його прийому використовують спеціальні приймачі з високою чутливістю. Фільтри встановлюються для виключення впливу зондувального та перевідбитого сигналів. Цей канал часто використовується для перехоплення розмов, які переходять межі контрольованої зони через телефонні апарати, і включає спеціальні заходи, такі як встановлення високочастотних фільтрів, щоб уникнути впливу на апаратуру АТС в лінію, що йде в її бік.

1.2.4 Оптико-електронний канал витоку інформації

Оптико-електронний або лазерний канал витоку акустичної інформації формується шляхом опромінення лазерним променем тонких поверхонь, таких як скло вікон, картин, дзеркала та інші. Ці поверхні вібрують під впливом акустичного поля. Відбите лазерне випромінювання, будь то дифузне або дзеркальне, модулюється як по амплітуді, так і по фазі відповідно до законів вібрацій поверхні. Модульоване випромінювання збирається приймачем оптичного (лазерного) сигналу. Під час демодуляції сигналу приймач виділяє мовну інформацію. Лазер та оптичний приймач можуть бути встановлені як в одному, так і в різних місцях, включаючи різні приміщення. Такий метод використовується для таємного отримання акустичних даних, використовуючи лазерні промені та вібруючі поверхні як несприятливий канал для витоку інформації.

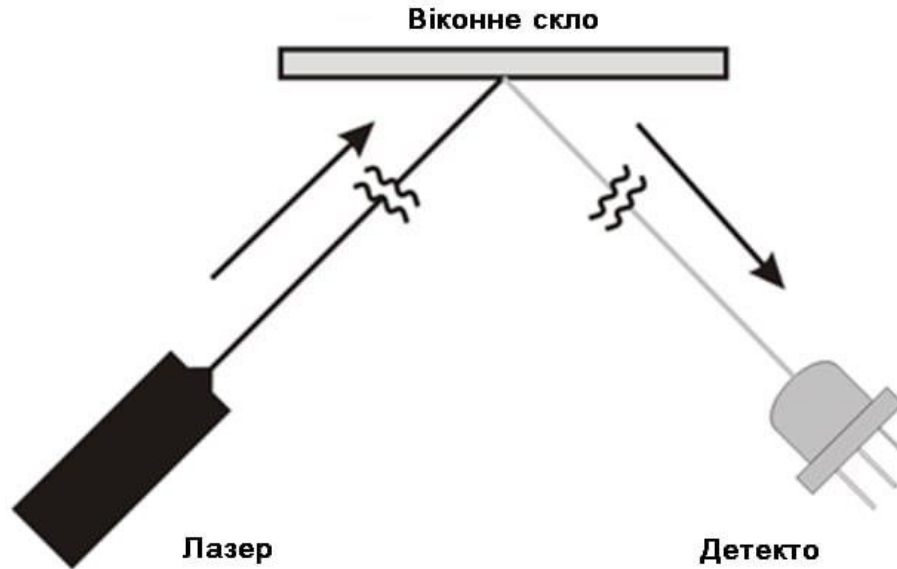


Рисунок 1.7 – Принцип дії ЛАРС

Для отримання мовної інформації через цей канал використовуються складні лазерні акустичні системи, відомі як "лазерні мікрофони". Ці системи зазвичай працюють у ближньому інфрачервоному діапазоні хвиль.

На малюнку зображено найпростіший варіант такої системи. Промінь лазера падає на скло вікна під деяким кутом. На кордоні скло – повітря відбувається модуляція променя звуковими коливаннями. Відбитий промінь уловлюється фотодетектором, розташованому на осі відбитого променя, здійснюється амплітудна демодуляція відбитого випромінювання. Система досить проста, але вимагає ретельного юстування і практично використовується досить рідко.

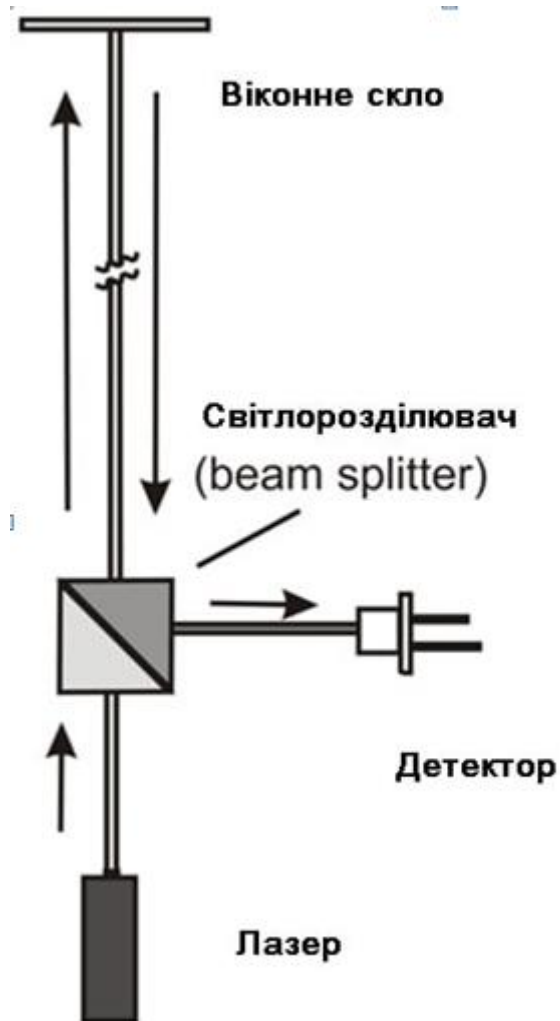


Рисунок 1.8 – Варіант схеми побудови ЛАСР із використанням спліттера (ділителя) пучка

Другий метод, в якому використовується спліттер пучка, є трошки складніший, але він дозволяє поєднати лазер і детектор (рис. 1.7). Цей підхід усуває необхідність в ретельному юстуванні системи. Застосування спліттера дозволяє зведення падаючого і відбитого променів в одну точку.

Для підвищення чутливості використовується інтерференційна схема, яку представлено на рисунку 1.8. Інтерферометр у цій схемі має плечі рівної довжини і відомий як "Dual Beam LASER Mic".

Основний принцип цієї схеми – це диференційний метод вимірювання акустичної вібрації. Ділянка шибки, з якої вимірюється вібрація, має невеликі

розміри, тому синфазна перешкода, викликана низькочастотними коливаннями скла, наприклад, від вітру або вуличного шуму, різко послаблюється.

1.2.5 Параметричний канал витоку інформації

Внаслідок впливу акустичного поля на високочастотні генератори ТСПІ та ДТЗС, тиск на їхні елементи змінюється, що призводить до незначних змін у їхньому розташуванні та параметрах. Це може викликати модуляцію високочастотного сигналу інформаційним сигналом, наприклад, через зміни в індуктивності чи ємності елементів. Такий канал витоку інформації відомий як параметричний.

Зміни в розташуванні проводів у котушках чи інших елементах можуть призвести до частотної модуляції сигналу. Наприклад, акустичне поле може впливати на відстань між пластинами конденсаторів, змінюючи їхню ємність, що в свою чергу може спричинити частотну модуляцію високочастотного сигналу генератора.

У технічному каналі витоку інформації через параметричні ефекти можлива паразитна модуляція високочастотних коливань, які випромінюються гетеродинами радіоприймачів. Ці зміни можуть бути перехоплені і виявлені радіорозвідувальними засобами. Параметричний канал може бути використаний, наприклад, для "високочастотного опромінення" приміщення з напівактивними заставними пристроями, які реагують на акустичні сигнали змінами своїх параметрів.

Для реалізації параметричного каналу витоку інформації може використовуватися "високочастотне опромінення" приміщення з напівактивними заставними пристроями, які мають елементи змінної ємності чи індуктивності. Застосування таких елементів призводить до утворення вторинних радіохвиль, а їх взаємодія зі спеціальними елементами закладки може викликати модуляцію сигналу відповідно до змін акустичного сигналу.

Подібні елементи закладки, в яких відбувається модуляція сигналу, іноді називають напівактивними. Для прийому інформації від цього каналу необхідні спеціальні приймачі, а також передавачі з направленою антеною.

2 РОЗРОБКА СИСТЕМИ ЗАХИСТУ

Для вирішення завдання ми будемо використовувати комплексний підхід. Для захисту мови від несанкціонованого прослуховування застосовують пасивні та активні методи.

2.1 Пасивні методи захисту

Пасивні методи захисту включають в себе заходи з ослаблення акустичних сигналів та обмеження продуктів електроакустичних перетворень, які поширюються в приміщенні через сполучні лінії ДТЗС. Це може відбуватися як природним шляхом, так і через нав'язування високочастотних сигналів.

Ослаблення акустичних сигналів досягається шляхом використання звукоізоляційних заходів для приміщень. Щодо передачі інформаційних електричних сигналів та сигналів високочастотного нав'язування, вони можуть бути фільтровані відповідними фільтрами. Активний захист може включати в себе використання генераторів перешкод, пристроїв для придушення та знищення.

Основна концепція пасивних засобів захисту полягає в тому, щоб зменшити співвідношення сигнал/шум в можливих точках перехоплення інформації. Це досягається зниженням інформативного сигналу, що вказує на важливість зменшення чутливості системи до небажаного перехоплення чи витоку інформації (рис. 2.1).

При виборі огорожувальних конструкцій для виділених приміщень у процесі проектування важливо керуватися рядом правил, спрямованих на покращення акустичного середовища:

- для перекриттів рекомендується використовувати матеріали або шари з різною звукопоглиблюючою здатністю;

- для підлоги рекомендується використовувати конструкції, які мають пружну основу або встановлені на віброізоляторах;
- стелі рекомендується виготовляти їх у вигляді підвісних конструкцій, що мають властивості звукопоглинання;
- для стін та перегородок важливо використовувати багатошарові акустично неоднорідні конструкції з пружними прокладками (гума, пробка, ДВП, і т.п.).

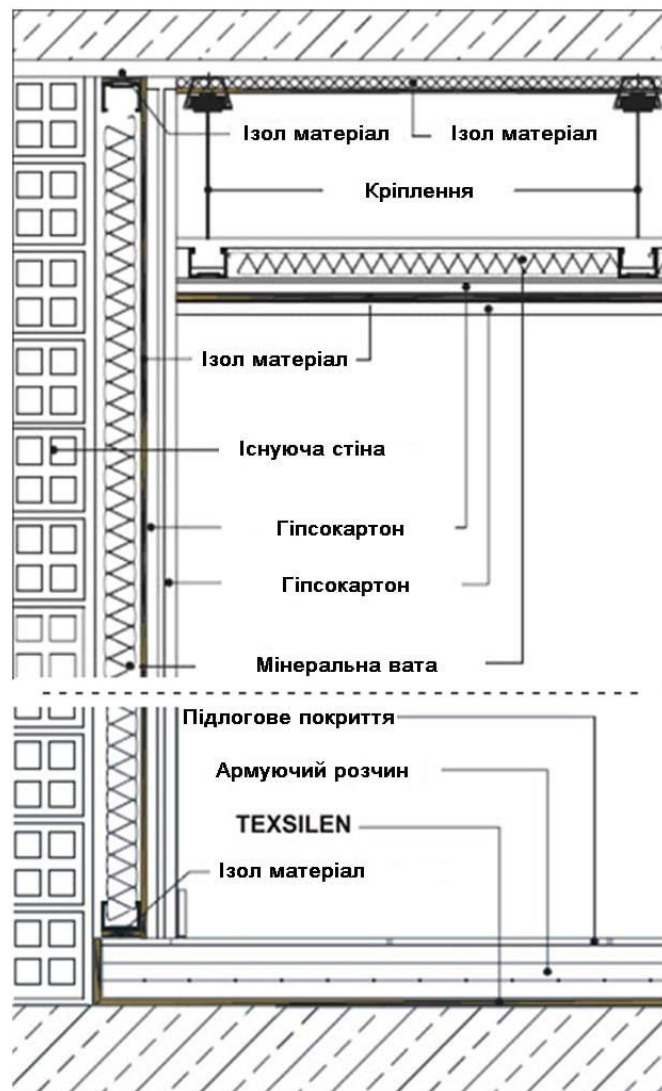
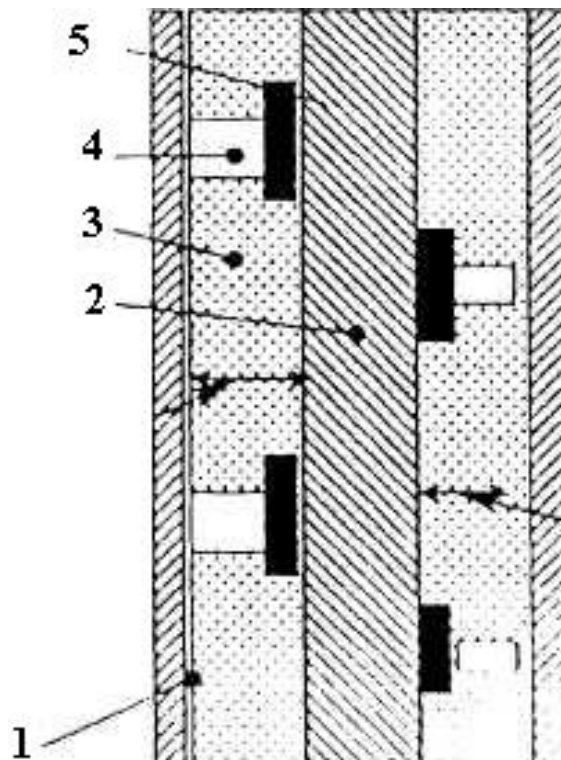


Рисунок 2.1 – Схема звукоізоляції приміщення

2.1.1 Звукоізоляція стін

В ситуації, коли стіни і перегородки мають одношарову акустично однорідну конструкцію, доцільно використовувати посилену конструкцію типу "плита на відносі". Це означає, що плита або панель буде встановлена із боку приміщення, з метою підвищення її акустичної ефективності (рис. 2.2).



1 – віднесена плита; 2 – конструкція, що несе; 3 – звукопоглинаючий матеріал; 4 – обрешітка; 5 – віброізолятор.

Рисунок 2.2 – Схема пасивного захисту стіни

2.1.2 Звукоізоляція стелі

Облицювання стель здійснюється звукопоглинаючими матеріалами з перфорованим покриттям та без перфорованого покриття. Як облицювальні

матеріали використовуються мінераловатні плити з ненаскрізною перфорацією. Можуть використовуватися гіпсокартонні та дерев'яні матеріали. Застосування звукопоглинаючих облицювань стель дозволяє забезпечити зниження рівня сигналу на величину до 6 дБ.

2.1.3 Звукоізоляція підлоги

Підвищення звукоізоляції приміщень у бік підлоги досягається покриттям чорної підлоги паркетом або дошками білої підлоги. Під лаги, на які кріпиться.

«Біла підлога» – підкладаються прокладки з губчастої гуми. Розмір повітряного зазору між підлогами вибирається щонайменше 50-100 мм. Додатково підлога може бути обладнана килимовими покриттями.

2.1.4 Екранування вентиляційних отворів

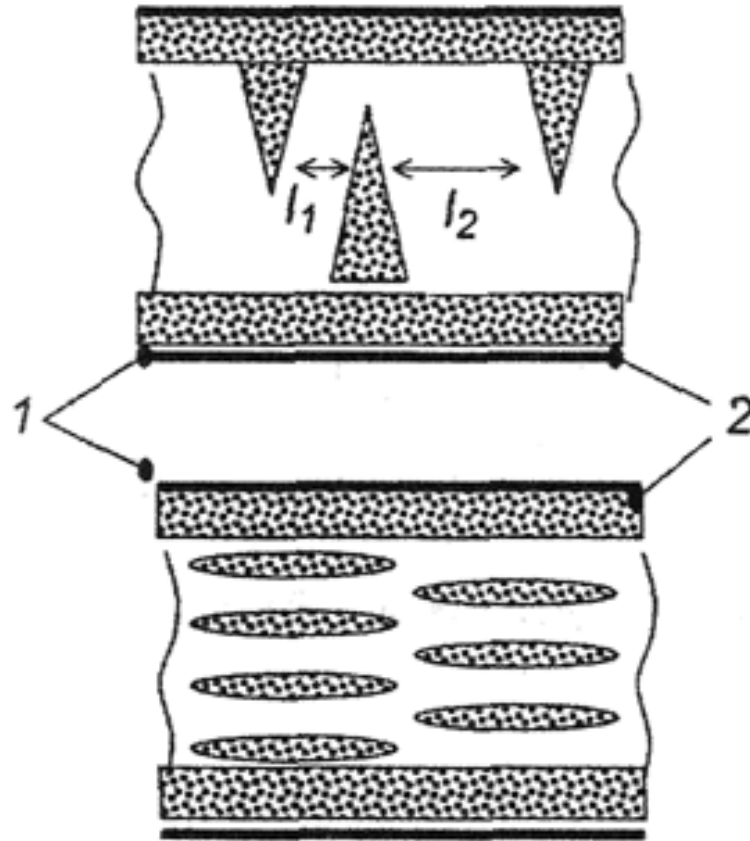
Ефективність екранування вентиляційних отворів залежить від відношення геометричних розмірів екрану та отвору та величини повітряного зазору між екраном та отвором (рис. 2.3).

Оптимальним вважається, коли геометричні розміри екрану більше розмірів отвору не менше ніж у три рази, а величина повітряного зазору приблизно в чотири рази менше діаметра отвору пружних прокладок та втулок.

2.1.5 Звукоізоляція вікон

Ущільнення скла віконних блоків проводиться за допомогою пружних прокладок з пористої або профільованої гуми. Ущільнення притворів включає щільне припасування всіх частин палітурок між собою і до коробки,

застосування ущільнюючих прокладок між палітурками і коробкою, застосування запірних пристроїв, що забезпечують щільне закриття.



1 – стінки короба вентиляції; 2 – звукопоглинаючий матеріал.

Рисунок 2.3 – Звукоізоляція короба вентиляції

Ущільнення скла і палітурки дозволяє збільшити звукоізоляцію віконних прорізів на 5-10 дБ. Облицювання периметра міжскляного простору здійснюється пористими звукопоглинаючими матеріалами, наприклад, повсть або мінеральне волокно, під які можуть додатково підкладатися перфоровані екрани, наприклад, з листового алюмінію. Товщина облицювання – 30...50 мм. Облицювання периметра міжскляного простору дозволяє збільшити звукоізоляцію віконних прорізів в середньому на 5 дБ.

Спеціальні конструкції віконних блоків передбачають встановлення подвійного та потрійного скла, а також збільшення повітряного міжскляного зазору.

В таблиці 2.1 наведено довідкові дані щодо звукоізоляції віконних рам.

Таблиця 2.1 – Довідкові дані щодо звукоізоляції віконних рам

Конструкція	Примітка	Звукоізоляція (дБ) на частотах, Гц				
		250	500	1000	2000	4000
Віконний блок з подвійною палітуркою, товщина скла 3 мм, повітряний зазор 170 мм	без прокладок	26	28	30	28	27
	з прокладками із пористої гуми	33	36	38	38	38
Віконний блок з подвійною палітуркою, товщина скла 4 мм	повітряний зазор 100мм, з герметизацією притвору	35	39	47	46	52
	повітряний зазор 200мм, з прокладками	36	41	47	49	55
	повітряний зазор 300мм, з прокладками	39	43	47	51	55
Склопакет, товщина 98 мм	з прокладками	40	42	45	48	50

Для захисту від лазерних мікрофонів із зовнішнього боку вікон встановлюють шибки з рифленою поверхнею. При установці звичайного скла

їм надається кут нахилу, що виключає можливість виходу відбитого променя до місця можливого розташування розвідувального пункту (рис. 2.4).

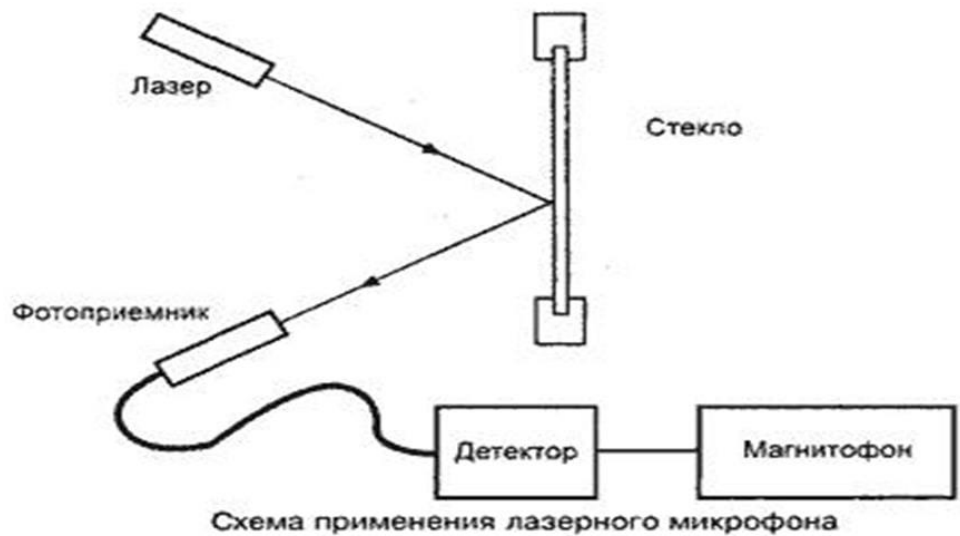


Рисунок 2.4 – Схема застосування лазерного мікрофона

2.1.6 Звукоізоляція дверей

Двері для виділених приміщень повинні бути подвійними з тамбуром і з двома коробками, між якими повинна бути вібраційна розв'язка (рис. 2.5).

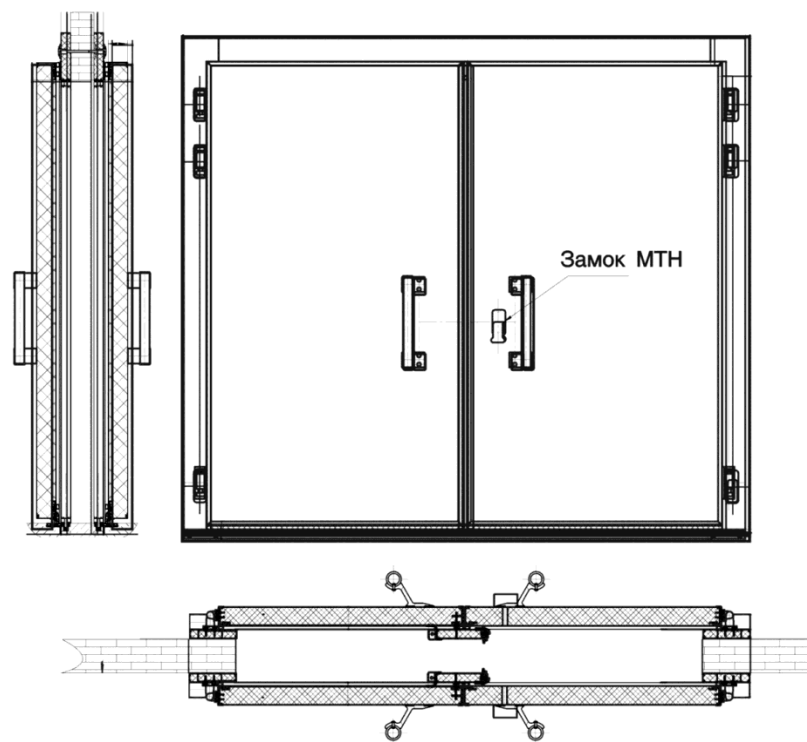


Рисунок 2.5 – Зображення двохтамбурних дверей

2.1.7 Інтер'єр

Окрім проведення розглянутих вище інженерно-будівельних заходів додаткової звукоізоляції приміщень можна домогтися відповідним обладнанням внутрішнього інтер'єру, наприклад, завішуванням вікон важкими плюшевими або оксамитовими портьєрами, обстановка приміщення м'якими меблями з оббивкою зі звукопоглинаючого матеріалу, покриття підлог вовняними килимами або доріг. Так наприклад ефективна звукопоглинаюча поверхня м'якого крісла з наповнювачем з в'язкого матеріалу приблизно в десять разів більша за ефективну звукопоглинаючу поверхню стільця з жорстким сидінням і спинкою.

Виконання вищезгаданих заходів дозволяє підвищити звукоізоляцію приміщень на 3-6 дБ.

В таблиці 2.2 наведено значення коефіцієнта звукопоглинання різних типів матеріалів залежно від частоти.

Таблиця 2.2 – Значення коефіцієнта звукопоглинання різних типів матеріалів залежно від частоти

Коефициент поглощения						
Материал	Полосы частот					
	125 Hz	250 HZ	500 HZ	1 kHz	2 kHz	4 kHz
Вода (бассейн)	0.01	0.01	0.01	0.01	0.01	0.02
Цемент	0.02	0.02	0.02	0.03	0.04	0.04
Гипсовые панели	0.03	0.04	0.03	0.03	0.04	0.04
Дерево	0.15	0.20	0.10	0.10	0.05	0.05
Кирпичная стена	0.05	0.04	0.02	0.04	0.05	0.05
Стекло	0.30	0.20	0.10	0.07	0.05	0.02
Паркет	0.10	0.25	0.10	0.10	0.05	0.05
Пластик	0.03	0.04	0.05	0.05	0.08	0.05
Ковер	0.05	0.10	0.30	0.50	0.05	0.70
Пустое мягкое кресло	0.15	0.25	0.35	0.40	0.45	0.35
Мягкое кресло с человеком	0.25	0.40	0.55	0.05	0.65	0.60
Стекловата	0.20	0.45	0.70	0.80	0.80	0.80
Публика (м ²)	0.40	0.60	0.80	0.90	0.90	0.80
Пенополиуретан	0.15	0.40	0.95	1.00	1.00	1.00

2.2 Активні засоби захисту приміщень

Активні методи захисту приміщень передбачають використання різноманітних засобів для створення перешкод та знищення можливостей витоку конфіденційної інформації через віброакустичний канал. Основні елементи цього каналу включають джерела конфіденційної інформації, середовище розповсюдження (такі як повітря та огорожувальні конструкції приміщень), а також засоби знімання, такі як мікрофони та стетоскопи.

Для захисту використовуються різні технології, такі як генератори білого або рожевого шуму, генератори шуму речоподібного та системи вібраційного зашумлення. Генератори шуму можуть створювати випадковий або псевдовипадковий шум для перешкодження акустичним сигналам. Системи вібраційного зашумлення використовують віброперетворювачі для створення вібрацій у структурах, таких як стіни або підлога, щоб приглушити або маскувати звукові коливання.

Ефективність цих систем визначається перевищенням інтенсивності маскуючого впливу над рівнем акустичних сигналів в середовищах. Це перевищення регулюється нормативами та стандартами, визначеними відповідними керівними документами, зокрема Службою безпеки України

2.3 Організаційні заходи під час проведення нарад

Проведення нарад з участю представників сторонніх організацій вимагає попереднього дозволу директора, який призначає відповідальну особу за організацію цього заходу. Відповідальна особа спільно з представниками служби безпеки та технічними спеціалістами виконує необхідні заходи, спрямовані на забезпечення конфіденційності обговорюваних питань.

Порядок розгляду питань на нараді встановлюється таким чином, щоб учасники мали відношення до обговорюваних тем. Відповідальна особа готує проект програми наради та список учасників, в якому детально вказується інформація про кожного учасника, включаючи місце роботи, посаду та питання, в обговоренні яких вони можуть брати участь.

Учасники допускаються на нараду лише за наявності документів, що підтверджують їх особу. Заходи щодо захисту інформації на нараді спрямовані на підготовку відповідного приміщення та запобігання можливому витоку інформації, з урахуванням особливостей проведення самої наради.

Під час проведення нарад рекомендується вживати наступні організаційні заходи:

- перед тим як проводити нараду слід ретельно перевірити приміщення на предмет наявності заставних пристроїв. Огляд повинен бути систематизованим та проводитися спільно з представниками служби безпеки та особами, які добре знають обстановку;

- охорона має оглядати прилеглі приміщення перед нарадою, перевіряючи їх на наявність осіб, які можуть вести підслуховування. - кількість осіб, які беруть участь у конфіденційних переговорах, повинна бути обмежена до мінімуму;

- забороняється доступ до цих приміщень під час наради;

- кількість осіб, які беруть участь у конфіденційних нарадах, має бути обмеженою;

- розглянути можливість перенесення нарад на неробочий час для зменшення ризику витоку інформації;

- всі роботи в приміщенні, що проводяться поза часом наради, повинні здійснюватися в присутності представника служби безпеки;

- після наради проводити ретельний огляд, закривати та опечатувати приміщення.

Вказані організаційні заходи є дієвими та відносно легко впроваджуваними, а також можуть взаємодіяти для створення комплексної системи захисту конфіденційної інформації в приміщенні для нарад. Вони враховують різні аспекти, починаючи від забезпечення безпеки самого приміщення і закінчуючи контролем доступу та запобіганням можливих загроз.

З РОЗРОБКА СТРУКТУРНОЇ СХЕМИ УПРАВЛІННЯ ЗАХИСТОМ

Основна задача полягає в тому, щоб система була безперебійною та дистанційно керувалася. Потрібне електрозабезпечення та електричні автомати на кожен пристрій. Щоб керувати приборами для акустичного захисту знадобиться релейний модуль з керуванням по Ethernet, він буде керувати живленням приладів. Для дистанційного керування модулем реле необхідно підключити до локальної мережі з можливістю розмежування доступу для персоналу, який відповідає за безпеку даного приміщення. Для віддаленого контролю обстановки у приміщенні та можливості управління з головного офісу (у разі коли конференс зал знаходиться у філії підприємства), необхідно організувати безперебійний доступ до даного обладнання шляхом резервування каналів зв'язку.

Для моніторингу обстановки у приміщенні та поза ним встановлюється відеоспостереження. Бажано, щоб одна з камер мала вбудований мікрофон для можливості контролю працездатності генератора звукових шумів. Знаходження однієї з камер повинно бути так, щоб спостерігати працездатність обладнання.

Відповідальна людина буде дивитися за периметром та вмикати шумові генератори на початку переговорів. Спостерігати за камерами він буде через веб-інтерфейс (рис. 3.1), а вмикати акустичний захист через програму вмикання реле (рис. 3.2).

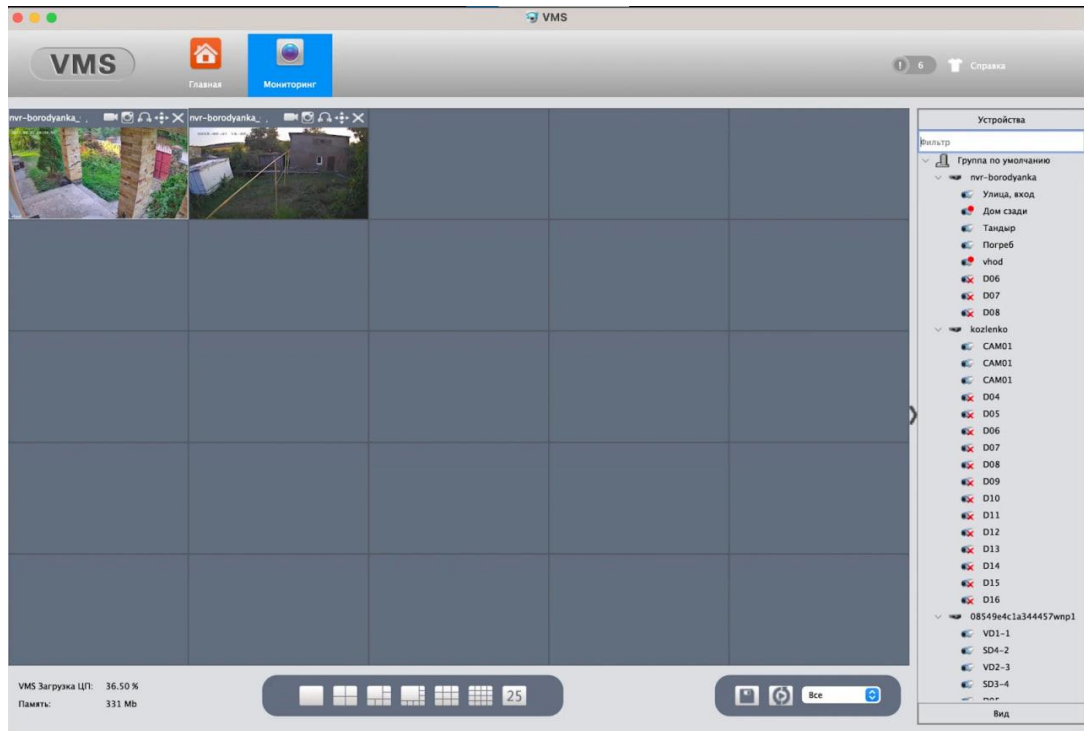


Рисунок 3.1 – Зображення веб-інтерфейсу камер спостереження

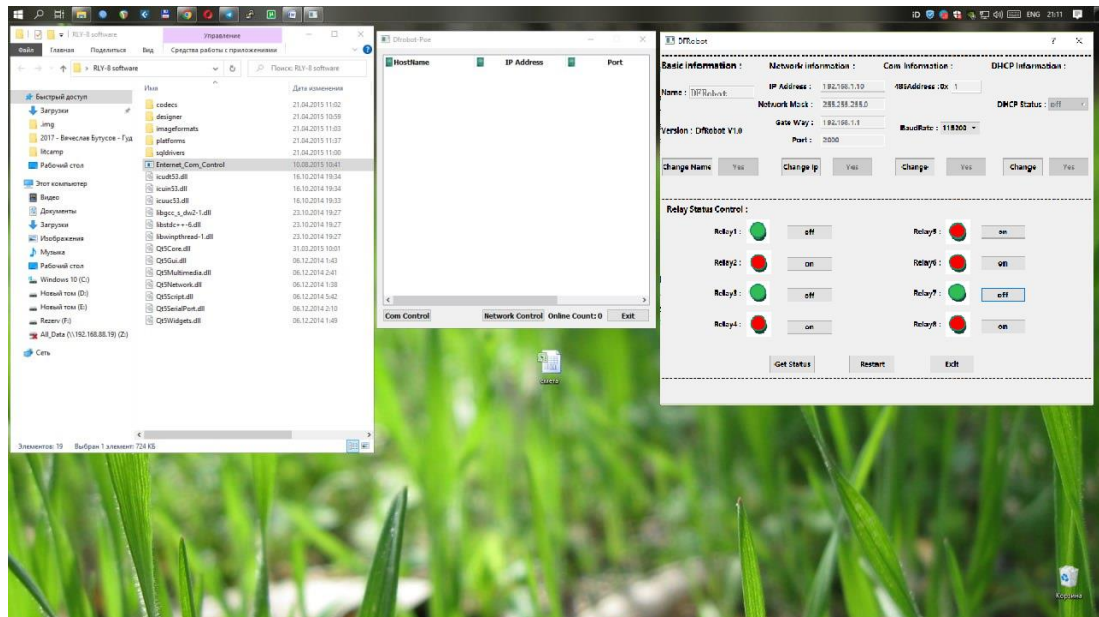


Рисунок 3.2 – Зображення програми вмикання реле

Для підвищення стійкості до відмов системи потрібно організувати безперебійне живлення. Шляхом встановлення ДБЖ з необхідним об'ємом

аккумуляторних батарей. Так само з метою підвищення стійкості системи перед кожним приладом в ланцюзі живлення встановлюється автоматичний вимикач. Щоб убезпечити себе від сценарію, коли один прилад викликає коротке замикання, внаслідок чого ДБЖ вимикає повністю всю апаратуру, встановлену в шафі. На рисунку 3.3 зображено структурну схему підключення приладів.

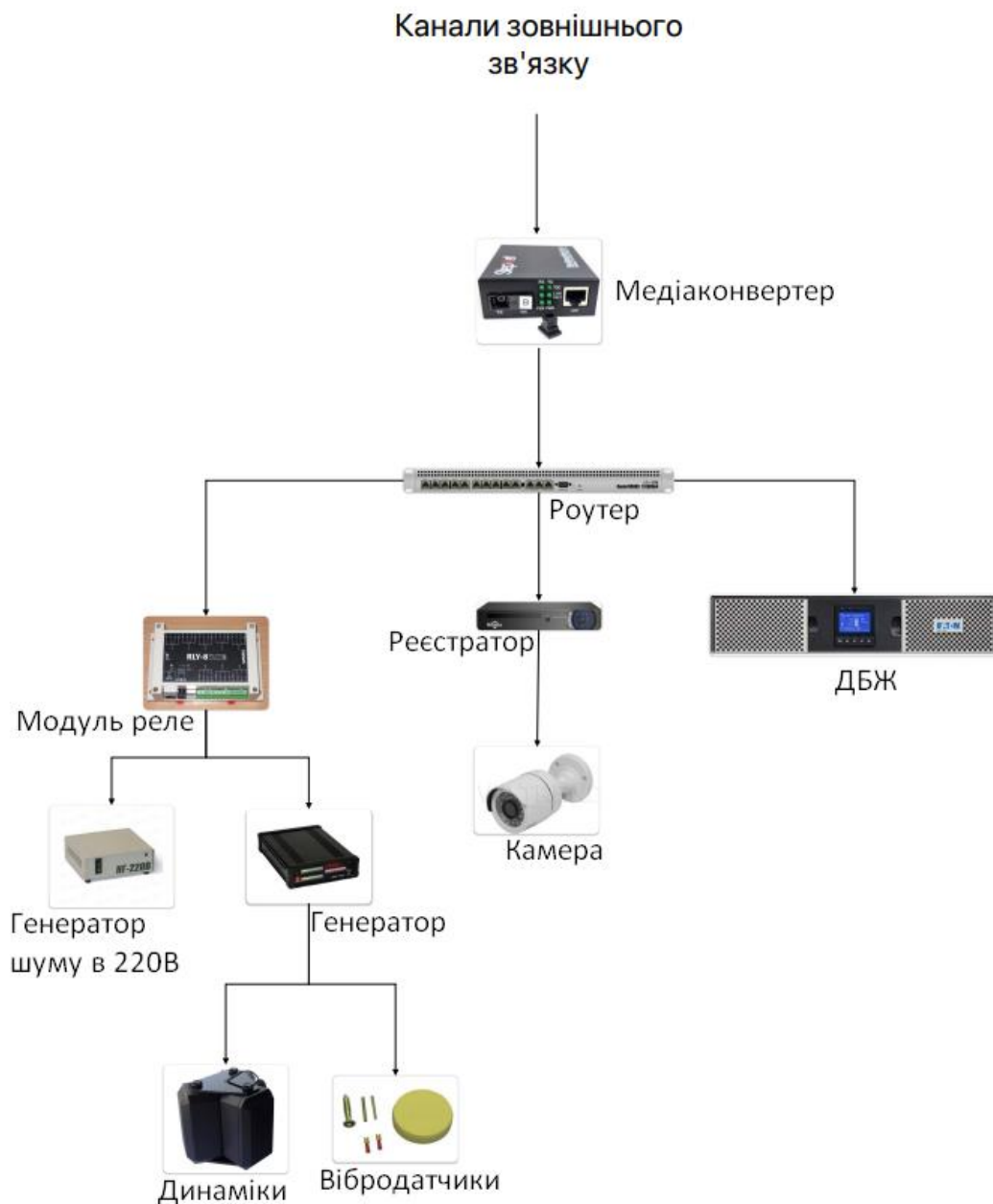


Рисунок 3.3 – Структурна схема підключення приладів

На рисунку 3.4 зображено стійку з розташуванням обладнання.

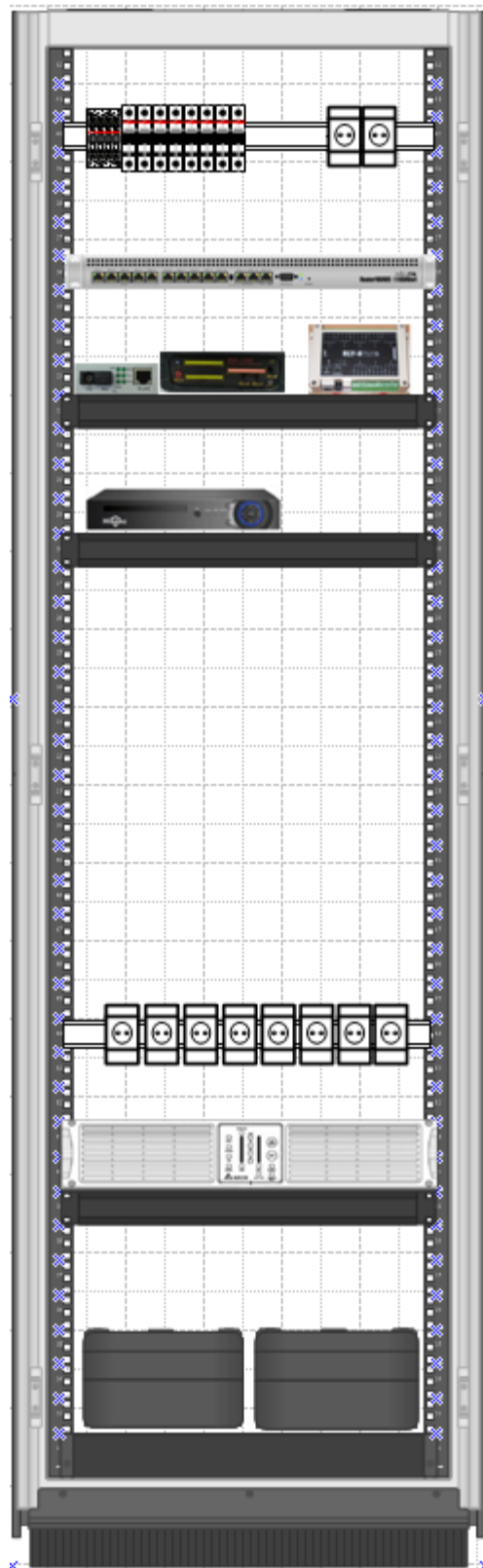


Рисунок 3.4 – Стійка з обладнанням

4 ВИБІР ОБЛАДНАННЯ

4.1 Вибір провайдера

Задача резервування каналів зв'язку реалізується з шляхом укладання договорів з кількома провайдерами підключеними по оптичному каналу передачі даних і мобільним gsm оператором. Підключення провайдерів по мідним проводам не бажано, оскільки існує ризик виходу з ладу встановленої апаратури в грозу.

4.1.1 Відмінності GERON і EPON

GERON і EPON ідентичні за винятком швидкості і створені за одним стандартом IEEE 802.3ah, а GPON – принципово інша технологія на основі стандарту ITU-TG.984.

У GERON пакетна передача Ethernet здійснюється PON-мережами в початковому вигляді. Передача в GPON базується на дворівневій інкапсуляції. Спочатку телекомунікаційні потоки для телефонії та Ethernet перетворюються в GEM-кадри за загальною процедурою фреймування (GFP), у цьому форматі передбачена змінна довжина корисного навантаження. Далі АТМ-клітини та GEM-фрагментовані кадри за допомогою інкапсуляції трансформуються в GTC-кадри і далі вже йдуть в передачу по мережі PON. GEM- "упаковка" передбачає кадрову фрагментацію, а в GERON цього немає. Це є основною причиною зниження ефективності пропускної здатності.

4.1.2 Відмінності GPON і EPON

Швидкість. EPON в downstream та upstream досягає 1,25 Гбіт/с, GPON в downstream – до 2,488 Гбіт/с (з проміжними значеннями 155, 622 Мбіт/с,

1,244 Гбіт/с). Значення восходящих потоків наближається до швидкості 155, 622 Мбіт/с або 1,244 Гбіт/с.

Мережа абонента та дальність. Радіус EPON-мережі досягає 30 км. Структура пасивної PON-мережі представляє собою розгалуження з дерев 1х64. Топологічний ліс з деревами для GPON – це 1х128, а радіус не перевищує відстань в 20 км.

Логічне кодування. EPON розрахований на зайвисть коду 8/10В (кожні 8 символів замінюються на 10, що призводить до зниження ЕППЧ на 20%). У GPON – лінійне дворівневе кодування (NRZ), це метод примітивного біполярного кодування, який гарантує найменші втрати пропускну здатності з мінімальними втратами швидкості. ЕППЧ для EPON наближено до 70%, для GPON ефективність рідко коли буває менше 95%.

EPON (Ethernet Passive Optical Network) і GPON (Gigabit Passive Optical Network) є двома різними технологіями передачі даних через оптичне волокно, але вони мають кілька спільних характеристик.

Структура мережі. Обидві технології мають схожу структуру мережі, яка використовує поділ сигналу на декілька кінцевих підключень (PON – Passive Optical Network). PON має деревоподібну топологію, де одна лінія веде до кількох кінцевих абонентських пристроїв.

Запасна ділянка довжин хвиль. Обидві технології застосовують певні діапазони довжин хвиль, включаючи запасні ділянки для особливих послуг або мультимедійних потоків. Це дозволяє їм ефективно використовувати оптичне волокно для різноманітних цілей.

Хоча EPON і GPON поділяють кілька спільних рис, включаючи діапазони довжин хвиль і ключі шифрування, вони також відрізняються за швидкістю і деякими технічними особливостями. Вибір між ними схиляється в сторону GPON.

4.2 Вибір медіа конвертору

Медіаконвертор – це пристрій, спеціально створений для передачі даних та перетворення їх між різними середовищами передачі. Якщо взглянути на приклад компанії, що вирішила розширити свою мережу, тоу цьому випадку ідеальним рішенням, яке враховує як вартість, так і якість, може стати використання медіаконвертера.

Компанія вже використовує оптоволоконний зв'язок для частини своєї мережі, але тепер їй потрібно підключити нові області. Замість того, щоб змінювати всю існуючу інфраструктуру, компанія може використати медіаконвертер для забезпечення зв'язку між оптоволоконними і мідними ділянками мережі.

Медіаконвертор дозволяє оптимізувати мережу, в якій використовуються мідні кабелі, адаптуючи їх до потреб оптичного зв'язку. Це важливо для ефективного збільшення пропускної здатності та розширення мережі. Пристрій просто трансформує сигнали між медними та оптичними ділянками, забезпечуючи високоякісне та надійне з'єднання між різними елементами мережі.

В якості обладнання для перетворення оптичного сигналу в електричний був обраний Медіаконвертор Step4Net MC-R-0,1-1SM-1550nm-20 (рис. 4.1). Медіаконвертор Step4Net призначений для перетворення сигналу зі стандарту 10BASE-T/100BASE-TX Fast Ethernet на кручений парі в сигнал стандарту 100BASE-FX Fast Ethernet по одномодовому оптоволокну.

Підтримуючи технологію WDM, медіаконвертори Step4Net дозволяють одночасно передавати та отримувати сигнали на довжині хвилі 1550 нм по одному оптичному волокну на відстань до 20 км.



Рисунок 4.1 – Зображення медіа конвертору Step4Net

Характеристики медіа конвертору:

- тип волокна: SM (Singlemode);
- мережеві інтерфейси: RJ45 100 Мбіт/с SC;
- джерело живлення: адаптер живлення: 5В, 1А;
- розміри: 94 x 70 x 26 мм;
- довжина хвилі, нм: 1550;
- робоча дистанція: 20км;
- тип конектора: SC;
- інтерфейси: RJ-45;
- швидкість передачі даних: 100 Мб/с.

4.3 Вибір роутеру

Основний критерій у виборі роутеру є наявність апаратного шифрування, бо це важливо для забезпечення безпеки та конфіденційності даних, особливо при передачі інформації через мережу. Ось кілька основних причин, чому апаратне шифрування в роутері може бути необхідним.

Безпека даних. Апаратне шифрування забезпечує більш високий рівень безпеки даних, ніж програмне забезпечення. Процесори, спеціально розроблені для обробки шифрування, можуть ефективно забезпечувати захист даних, роблячи їх менш уразливими до зовнішніх атак.

Продуктивність. Апаратне шифрування може значно підвищити продуктивність мережевих пристроїв, таких як роутери. Спеціалізовані шифрувальні процесори здатні обробляти шифрування даних більш ефективно та швидко, що особливо важливо у мережах з високим навантаженням.

Захист від атак. Апаратне шифрування знижує рівень вразливості перед атаками, такими як атаки шляхом перебору паролів або злому шляхом зворотної розробки програмного коду. Процеси, реалізовані на апаратному рівні, найчастіше складніше піддаються злому.

Широкосмуговий захист. Апаратне шифрування може забезпечити захист на більш високих рівнях мережного стека, забезпечуючи шифрування даних на рівні передачі даних, сесій або навіть прикладного рівня.

Дотримання стандартів безпеки. У різних секторах, таких як банківська сфера, охорона здоров'я або державні установи, можуть існувати стандарти безпеки, які вимагають використання апаратного шифрування для дотримання регулювань та нормативів.

MikroTik RB1100AHx4 (рис. 4.2) з 13 гігабітними портами Ethernet для мережі – це пристрій, що працює на потужному процесорі Annapurna Alpine AL21400 з чотирма ядрами Cortex A15, кожне з яких має тактову частоту 1,4 ГГц. Цей роутер має вражаючу максимальну пропускну здатність

до 7,5 Гбіт, що робить його відмінним вибором для високопродуктивних мереж.



Рисунок 4.2 – Зображення Mikrotik RB1100AHx4

Характеристики роутеру:

- архітектура: ARM 32 bit;
- ЦП: AL21400;
- кількість ядер: ЦП 4;
- номінальна частота процесора: 1,4 ГГц;
- модель мікросхеми комутатора: RTL8367;
- розміри: 443 x 148 x 44 мм;
- ліцензія: RouterOS 6;
- операційна система :RouterOS;
- розмір оперативної пам'яті: 1 Гб;
- розмір пам'яті: 128 Мб;
- тип накопичувача: NAND.

Випробувана температура навколишнього середовища від -40°C до 70°C.

Особливо слід відзначити його підтримку апаратного прискорення IPsec, яке може досягати швидкості до 2,2 Гбіт/с з AES128. Це важливо для забезпечення безпеки мережі, особливо при використанні віддалених з'єднань та VPN.

RB1100AHx4 постачається в корпусі для монтажу в стійку 19 дюймів та займає 1 юніт, що робить його зручним для використання в центрах обробки даних чи інших великих мережевих середовищах. Також варто відзначити послідовний порт RS232 та подвійні резервні джерела живлення, що роблять його надійним та готовим до використання в різних умовах, включаючи телекомунікаційне живлення.

Цей роутер також підтримує стандарт 802.3at/af для живлення пристроїв через Ethernet, що може бути зручно при підключенні пристроїв, таких як IP-камери чи точки доступу.

Загалом, MikroTik RB1100AHx4 забезпечить високу продуктивність та надійність для мережі, і відмінно впишеться в потреби сучасного підприємства чи організації.

4.4 Комплект відеоспостереження

В данному випадку камери потрібні для того щоб відстежувати працездатність всієї системи дистанційно та для того щоб поставити по периметру для моніторингу ситуації поза приміщенням. Для цього підійде реєстратор Hiseeu (рис. 4.3) з набором IP-камер Hiseeu (рис. 4.4) 4Мп 3,6мм. Є можливість використовувати жорсткий диск комп'ютера форм-факторів 2,5" або 3,5" з підтримкою SATA та об'ємом до 14 ТБ, який встановлюється всередині корпусу реєстратора (жорсткий диск не входить в комплект постачання). Підтримка кодування відеофайлів H.265 забезпечує максимальну економію місця на жорсткому диску. Ви також можете виконувати резервне копіювання будь-якого відрізка запису на флеш-накопичувач через інтерфейс USB.

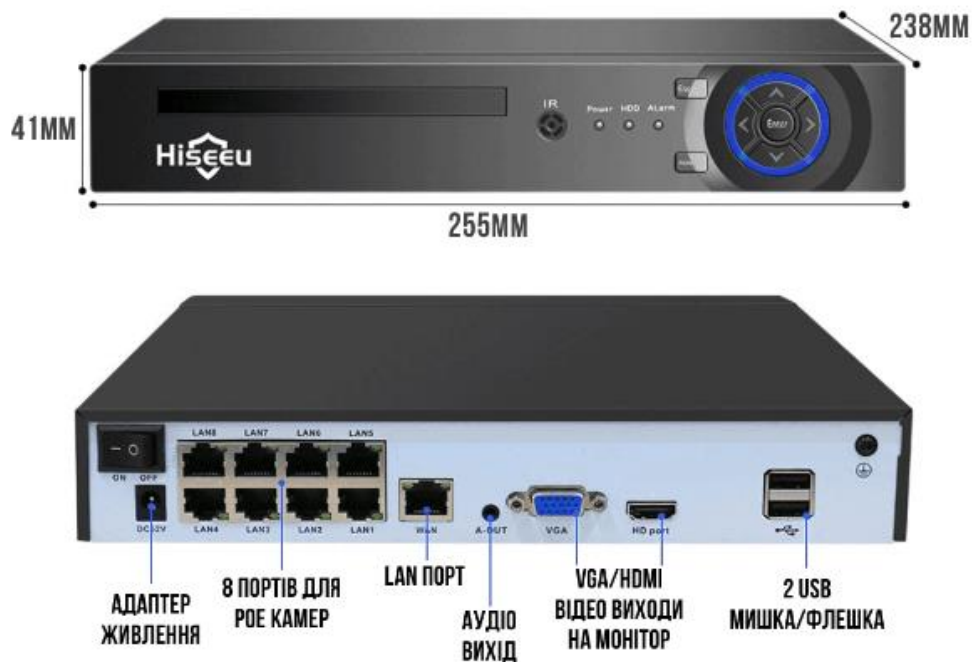


Рисунок 4.3 – Зображення відеореєстратору HiSeeu

4.4.1 IP відеореєстратор HiSeeu

Технічні характеристики реєстратора HiSeeu:

- підтримка до 8 IP камер;
- операційна система – Embedded LINUX;
- диски, що підключаються - 1 sata HDD до 14 тб;
- мережевий вхід – 1 Ethernet 100Mbps;
- HDMI/VGA виходи для підключення монітора (максимальна роздільна здатність 2560x1440);
- режими перегляду відео потоку 1/4/8 камер одночасно;
- вихід Sata та живлення для жорсткого диска (шнури в комплекті);
- 2 usb виходу (для підключення мишки, накопичувача для копіювання архіву запису);
- 8 PoE 48v портів LAN;

- 24 мови меню, у тому числі ru/eng;
- габарити: 22,2 x25, 5см;

Комплектація:

- IP Камера Hiseeu 4мп 3,6мм - 4шт;
- кріпильні шурупи із дюбелями для кожної камери;
- вологозахисні ковпачки для конекторів RJ45 для кожної камери;
- PoE IP Реєстратор Hiseeu 8-портовий 48v;
- блок живлення для реєстратора;
- Ethernet PoE кабель вуличний 20 метрів для кожної камери;
- Ethernet кабель для підключення реєстратора до роутера 50см;
- HDMI кабель для підключення реєстратора до монітора чи телевізора;
- мишка комп'ютерна;
- гвинти кріплення жорсткого диска HDD;
- посібник користувача для реєстратора;

4.4.2 IP Камери Hiseeu 4MP

Технічні характеристики IP Камери Hiseeu 4MP (рис. 4.4):

- металевий циліндричний корпус зі ступенем пиловологозахисту IP66;
- модуль на базі матриці 1/2.7" Smartsens 4MP (Роздільна здатність: 2688x1520);
- універсальний 3,6mm/f1.2 об'єктив з нічним ІЧ-фільтром та кутом огляду 90 градусів по горизонталі;
- відео компресія: H.265;
- AI Аналітика: Виявлення руху / Виявлення силуету людини (в заданій області в т.ч. перетин лінії) / Виявлення особи людини;
- мікрофон для запису аудіо;

- POE 48v модуль для передачі даних та живлення одним LAN кабелем;
- нічна Ік-підсвічування з 3 Ік-діодами, що забезпечують видимість у темряві до 25 метрів.



Рисунок 4.4 – Зображення ІР Камери HiSeeu

4.5 Вибір реле

Релейний модуль потрібен для дистанційного вмикання та вимикання акустичного захисту.

RLY-8 (рис. 4.5) – це мережеве реле-контролер з відкритим протоколом спілкування. На платі розміщено 8 реле, кожне з яких витримує 277В/10А або 125В/12А змінних. Оскільки більша частина побутової техніки працює на 220В, то даний пристрій підійде майже всюди.



Рисунок 4.5 – Зображення релейного модулю з керуванням по Ethernet RLY-8

RLY-8 створена на базі мікроконтролера STM32, підтримує 2 типи живлення (від розетки та через Ethernet-PoE). За рахунок останньої особливості пристрою, ви зможете зменшити кількість проводів. Крім того, керувати реле також можна через порт RS485 або TCP/IP протокол.

Дане Ethernet реле є чудовим вибором для проектів на базі Інтернету речей (IoT), а вісім механічних перемикачів дадуть вам простір, щоб постійно випробовувати щось нове. З відкритим та доступним всім протоколом, ви можете додати RLY-8 майже у будь який.

Особливості:

- відкритий протокол керування;
- можливість живлення від як від зовнішнього джерела так і від POE;
- 2 варіанти управління: Ethernet та RS485;
- є програмне забезпечення;

- відкритий USB протокол;
- відкритий JSON протокол;
- корпус промислового стандарту.

Характеристики:

- мікроконтролер: STM32;
- зовнішнє джерело живлення: 7-23 В (постійна напруга);
- живлення по POE: 44-57 В (постійна напруга);
- максимальна потужність перемикання: 10А/277В (змінна напруга) або 12А/125В (змінна напруга);
- мережева конфігурація: DHCP/Static IP Address;
- керування навантаженням: Ethernet/USB;
- IP по замовчуванню: 192.168.1.10 (Port:2000);
- робоча температура: -30 до +85° С;
- розмір: 145ммх90ммх40мм;
- вага: 530 г.

4.6 Вибір активних акустичних завад

Для акустичного захисту DNG-2300 (рис. 4.6) є оптимальним та передовим пристроєм для захисту приміщення від зовнішнього прослуховування, тобто від використання лазерних зчитувачів, зовнішніх напрямлених мікрофонів, прослуховування через вентиляційні шахти тощо. Це триканальний генератор акустичного "білого" шуму з двома каналами "вібро" та одним каналом "акусто".

Він використовується разом із вібровипромінювачами TRN-2000 (рис. 4.7) та акустичними випромінювачами OMS-2000 (рис. 4.8). Пристрій може створювати перешкоди для диктофонів та інших слухових пристроїв, розташованих всередині приміщення.



Рисунок 4.6 – Генератор акустичного шуму DNG-2300

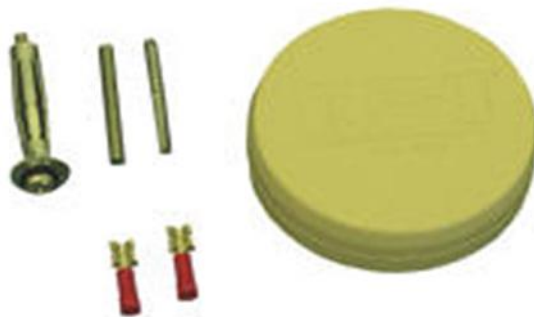


Рисунок 4.7 – Датчики TRN-2000

Характеристики TRN-2000:

- розмір: 101 x 38 мм;
- вага: 907 г;
- опір: 6 Ом.



Рисунок 4.8 – Динаміки OMS-2000

Характеристики динаміків OMS-2000:

- кількість динаміків на генератор: 12;
- опір: 24 Ом;
- розмір: 12,7 x 14,6 см;
- вага: 500 г.

Мережевий генератор шуму Рубіж НГ (рис. 4.9) призначений для придушення пристроїв, що підслухують, використовують як канал передачі мережі 220 В.



Рисунок 4.9 – Генератор шуму Рубіж НГ

Він забезпечує генерацію шуму в діапазоні частотного діапазону від 300 Гц до 7 МГц. У діапазоні частот, що найчастіше використовується, від 25 кГц до 95 кГц генератор забезпечує максимальний рівень спектральної щільності потужності шумового сигналу. До країв діапазону рівень спектральної щільності потужності плавно знижується. Перешкода подається в мережу 220 В по шнуру живлення.

Технічні характеристики:

- ширина спектру шуму 300 Гц-7 МГц;
- спектральна щільність потужності в діапазоні:
 - а) 300 Гц-25 кГц $0,3 \cdot 10^{-2}$ мВт/Гц;
 - б) 25 кГц-95 кГц $2,8 \cdot 10^{-2}$ мВт/Гц;
 - в) 95 кГц-7 МГц $0,24 \cdot 10^{-3}$ мВт/Гц;
- потужність: 8,5 Вт;
- живлення: 220В, 50Гц.

4.7 Вибір ДБЖ

Головна мета безперебійного живлення полягає в тому, щоб постачати електроенергію для підключеної техніки у випадку, коли основна електромережа виходить з ладу. Це надає захист від можливих стрибків напруги, що можуть пошкодити електроніку та врятувати результати важкої праці чи взагалі функціонування приладів. Безперебійне живлення є важливим елементом для забезпечення надійності роботи електронного обладнання у випадку виникнення проблем з основним живленням.

ДБЖ DELTA R-Series 3kVA (UPS302R2002N035) – онлайн UPS з подвійним перетворенням для встановлення горизонтально/вертикально. Рекомендований для якісного електроживлення серверів, телекомунікаційного, мережного та медичного обладнання. UPS DELTA R-Series 3kVA (рис. 4.10) спеціально розроблений для безперебійного живлення відповідальних програм з великим часом автономної роботи. Для

ефективного заряду батареї великої ємності встановлено потужний зарядний пристрій. У комплект поставки входить кріплення для встановлення ДБЖ в 19 'стійку.



Рисунок 4.10 – Зображення ДБЖ DELTA R-Series 3kVA

ВИСНОВКИ

У цьому дипломному проєкті було розроблено та реалізовано дистанційну систему управління акустичного захисту конференц-залу. Ця система є інноваційним рішенням, яке забезпечує ефективне і гнучке управління акустичним середовищем в конференц-залі з віддаленої локації.

Основною метою проекту було створення системи, здатної автоматично та дистанційно регулювати параметри звукоізоляції у конференц-залі залежно від конкретних вимог та сценаріїв використання. Розроблена система дозволяє оптимізувати акустичне середовище для різних заходів, таких як конференції, лекції, презентації та інші.

Процес розробки включав проектування апаратної частини системи, розробку програмного забезпечення для управління та моніторингу, а також інтеграцію з існуючою інфраструктурою конференц-залу. Було враховано сучасні технологічні та акустичні вимоги, що дозволило створити стійку та ефективну систему.

Результати проведених тестів та експериментів підтвердили ефективність та надійність системи. Дистанційна система управління акустичним захистом конференц-залу успішно справляється з поставленими завданнями та демонструє потенціал для застосування у різних галузях.

На закінчення, дана дипломна робота дає приклад у область акустичних технологій і систем управління звуковим середовищем. Розроблена система обіцяє покращити комфортність та функціональність конференц-залів, надаючи оперативне та гнучке управління акустичним захистом з будь-якої віддаленої точки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Захист від прослуховування переговорів. [Електронний ресурс] – Режим доступу: <http://os-info.ru/enziklopedia-brzopasnosti/zashhita-ot-proslushivaniya-peregovorov.html> (дата звернення 29.09.2023). – Назва з екрану.
2. Інформаційна безпека. Технічні канали витоку акустичної (мовленнєвої) інформації [Електронний ресурс] – Режим доступу: http://shotgun.com.ua/inf_secur/tap_audio.html (дата звернення 15.10.2023). – Назва з екрану.
3. Хорев А.А. Засоби акустичної розвідки: спрямовані мікрофони та лазерні акустичні системи [Електронний ресурс]. – Режим доступу: <http://www.st-s.su/publications/2008/3/articles/horev/index.htm> (дата звернення 16.10.2023). – Назва з екрану.
4. Фізичні характеристики та сфера застосування матеріалу Texsilen [Електронний ресурс]. – Режим доступу: <http://www.tecsound.com.ua> (дата звернення 25.10.2023). – Назва з екрану.
5. Методи та засоби захисту телефонних апаратів та телефонних ліній [Електронний ресурс]. – Режим доступу: <http://kiev-security.org.ua/box/8/111.shtml> (дата звернення 25.10.2023). – Назва з екрану.
6. Рубіж НГ [Електронний ресурс]. – Режим доступу: <https://vesh.ua/rubezh-ng-setevoj-generator-shuma-dlja-setej-220-volt/> (дата звернення 2.11.2023). – Назва з екрану.
7. Генератор шуму DNG-2300 [Електронний ресурс]. – Режим доступу: <https://ibughunter.com.ua/uk/dng-2300/> (дата звернення 2.11.2023). – Назва з екрану.

8. Вібраційний випромінювач TRN-2000 [Електронний ресурс]. – Режим доступу: <https://ibughunter.com.ua/trn-2000-ru/> (дата звернення 2.11.2023). – Назва з екрану.

9. 8-канальне мережеве ethernet реле RLY-8 [Електронний ресурс]. – Режим доступу: <https://uamper.com/8-канальное-реле-ethernet-poe-коммутатор-DFRobot-rly8> (дата звернення 2.11.2023). – Назва з екрану.

10. Що таке PoE [Електронний ресурс]. – Режим доступу: <https://www.kirich.blog/obzory/bloki-pitaniya/592-что-такое-poe-na-primere-pary-kommutatorov.html> (дата звернення 5.11.2023). – Назва з екрану.

11. RB1100AHx4 [Електронний ресурс]. – Режим доступу: <https://mikrotik.com/product/rb1100ahx4> (дата звернення 7.11.2023). – Назва з екрану.

12. Технологія PON [Електронний ресурс]. – Режим доступу: <https://lantorg.com/ru/article/tehnologiya-pon-что-eto/> (дата звернення 7.11.2023). – Назва з екрану.

13. Медіаконвертер Step4Net [Електронний ресурс]. – Режим доступу: https://e-server.com.ua/uk/mediakonverter-step4net-mc-r-01-1sm-1550nm-20-ua?gad_source=1&gclid=Cj0KCQiAm4WsBhCiARIsAEJIEzUUPSeR6uRa1OwNXlvxbyrR_i4aPoDVVfNfgTbLszAnB73ocMgBtNEaApgcEALw_wcB (дата звернення 7.11.2023). – Назва з екрану.

14. Що являє собою медіаконвертер [Електронний ресурс]. – Режим доступу: <https://ru.nettech.ua/news/opticheskiy-mediakonverter-opisanie> (дата звернення 7.11.2023). – Назва з екрану.

15. POE Комплект відеоспостереження [Електронний ресурс]. – Режим доступу: https://xmeye.com.ua/ru/gotovye-komplekty-ip-videonablyudeniya/1986-poe-komplekt-videonablyudeniya-na-5-ip-kamer-hiseeu-4mp.html?gclid=Cj0KCQiAm4WsBhCiARIsAEJIEzW3Ywbt7r8DhRDhC4ltPx48otdusaG-XRBqt6qJQCvkYZ81SYp5QNMAt3XEALw_wcB (дата звернення 17.11.2023). – Назва з екрану.

16. ИБП DELTA R-Series 3kVA [Електронний ресурс]. – Режим доступу: <https://ipt-ups.com.ua/delta-r-series-3000va.html> (дата звернення 22.11.2023). – Назва з екрану.

17. Посібник користувача системи камери відеоспостереження Hiseeu PoE [Електронний ресурс]. – Режим доступу: <https://manuals.plus/ru/hiseeu/poe-security-camera-system-manual> (дата звернення 19.11.2023). – Назва з екрану.