

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

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Розробка пристрою захисту інформації від зйому мікрофоном направленої дії
акустичним каналом

Виконав: студент 4 курсу, гр.2КІТС-216
спеціальності 125– Кібербезпека
Освітня програма – Кібербезпека
інформаційних технологій та систем
(шифр і назва напрямку підготовки, спеціальності)



Соколовський Д.С.

(прізвище та ініціали)

Керівник: д.т.н., професор кафедри МБІС



Яремчук Ю.Є.

(прізвище та ініціали)

« 4 »

серпня

2025 р.

Рецензент: к.т.н., професор кафедри ОТ



Захарченко С.М.

(прізвище та ініціали)

« 4 »

серпня

2025 р.

Допущено до захисту

Голова секції УБ кафедри МБІС

д.т.н., професор Яремчук Ю.Є.

« 4 »

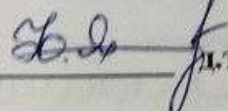
серпня

2025р.

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

Рівень вищої освіти I-й (бакалаврський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо-професійна програма - Кібербезпека інформаційних технологій та систем

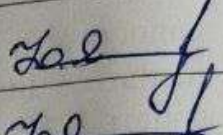
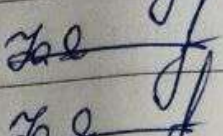
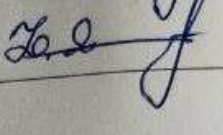
ЗАТВЕРДЖУЮ
Голова секції УБ, кафедра МБІС

 д.т.н., проф. Яремчук Ю.Є.
“ 20 ” березня 2025 р.

ЗАВДАННЯ
на бакалаврську кваліфікаційну роботу студенту
Соколовському Дмитру Сергійовичу
(прізвище, ім'я, по-батькові)

1. Тема роботи Розробка пристрою захисту інформації від зйому мікрофоном направленої дії акустичним каналом
Керівник роботи Яремчук Юрій Євгенович, д.т.н., професор кафедри МБІС
(прізвище, ім'я, по-батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від “20” березня 2025 року № 97
2. Термін подання студентом роботи 3 червня 2025р
3. Вихідні дані до роботи Електронні джерела, підручники та наукові статті по темі. Існуюче програмне забезпечення, яке стосується теми бакалаврської кваліфікаційної роботи.
4. Зміст текстової частини:
Для досягнення мети було поставлено такі задачі: здійснити дослідження загроз зйому інформації акустичним каналом за допомогою мікрофонів направленої дії; проаналізувати існуючі методи та пристрої захисту від подібних загроз; обґрунтувати вибір принципу дії та елементної бази пристрою для генерації акустичних завад; розробити алгоритм роботи пристрою та програмне забезпечення для його функціонування; зібрати прототип пристрою та провести експериментальні дослідження його ефективності.
5. Перелік ілюстративного матеріалу:
Презентація у форматі PowerPoint з ілюстраціями структурної схеми приладу та скріншотами моделювання схеми приладу

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ I	Яремчук Ю. Є., д.т.н., професор кафедри МБІС		
Розділ II	Яремчук Ю. Є., д.т.н., професор кафедри МБІС		
Розділ III	Яремчук Ю. Є., д.т.н., професор кафедри МБІС		

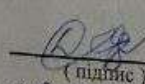
7. Дата видачі завдання 20 березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

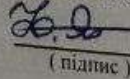
№	Назва та зміст етапу	Термін виконання		Примітка
		початок	закінчення	
1	Аналіз предметної області	01.04.2025	07.04.2025	Виконано
2	Аналіз методів розв'язання задачі	08.04.2025	14.04.2025	Виконано
3	Постановка задач розробки пристрою	15.04.2025	17.04.2025	Виконано
4	Дослідження інформаційних джерел	18.04.2025	21.04.2025	Виконано
5	Аналіз варіантів реалізації	22.04.2025	26.04.2025	Виконано
6	Розробка алгоритму роботи	27.04.2025	01.05.2025	Виконано
7	Реалізація програмного модулю	02.05.2025	05.05.2025	Виконано
8	Тестування програмного модулю	11.05.2025	10.05.2025	Виконано
9	Оформлення матеріалів до захисту БДР	21.05.2025	25.05.2025	Виконано

Студент

Керівник роботи


(підпис)

Соколовський Д.С.
(прізвище та ініціали)


(підпис)

Яремчук Ю.Є.
(прізвище та ініціали)

АНОТАЦІЯ

Дана бакалаврська кваліфікаційна робота присвячена розробці пристрою захисту інформації від зйому мікрофоном направленої дії акустичним каналом. В роботі проаналізовано існуючі загрози витоку інформації через акустичний канал та методи захисту від акустичного шпигунства. Визначено технічні аспекти для розробки пристрою, що ефективно захищає конфіденційні дані від витоку шляхом зйому інформації через акустичний канал.

У цій роботі наведено приклади захисту від витоку інформації акустичними та шляхами у приміщеннях та офісах, охарактеризовано особливості мікрофонів направленої дії та їхню небезпеку у контексті перехоплення даних. Також обґрунтовано доцільність використання активного методу захисту у вигляді генерації шумових завад у заданому частотному діапазоні.

Ключові слова: технічний захист інформації, акустичний канал, мікрофон направленої дії, генератор шуму, захист мовної інформації, акустичне шпигунство.

ABSTRACT

This bachelor's thesis is devoted to the development of a device for protecting information from being captured by a directional microphone through an acoustic channel. In the work the existing threats of information leakage through the acoustic channel and methods of protection against acoustic espionage are analyzed. The technical aspects for the development of a device that effectively protects confidential data from leakage by capturing information through an acoustic channel are determined.

This paper provides examples of protection against information leakage through acoustic and airborne channels in premises and offices, characterizes the features of directional microphones and their danger in the context of data interception. The expediency of using an active method of protection in the form of generating noise interference in a given frequency range is also substantiated.

Keywords: technical protection of information, acoustic channel, directional microphone, noise generator, protection of speech information, acoustic espionage.

ЗМІСТ

ВСТУП	8
1 ЗАГАЛЬНИЙ АНАЛІЗ СИСТЕМ ЗАХИСТУ ВІД АКУСТИЧНОГО ЗЙОМУ ІНФОРМАЦІЇ	10
1.1 Основні поняття та загрози зйому інформації акустичним каналом	10
1.2 Технічні засоби перехоплення інформації через акустичний канал	11
1.3 Дослідження існуючих технічних рішень	16
1.4 Мікрофони направленої дії: принцип роботи, чутливість та недоліки ...	19
1.5 Висновки до розділу 1 та постановка задачі	21
2 РОЗРОБКА ПРИСТРОЮ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ЗЙОМУ МІКРОФОНОМ НАПРАВЛЕНОЇ ДІЇ	23
2.1 Обґрунтування вибору технічного підходу	23
2.2 Обґрунтування вибору елементної бази	26
2.3 Обґрунтування вибору мови програмування	30
2.4 Структурна схема пристрою та сценарій його використання	32
2.5 Висновки до розділу 2	34
3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПРИСТРОЮ АКТИВНОГО АКУСТИЧНОГО ЗАХИСТУ	36
3.1 Реалізація програмного забезпечення пристрою.....	36
3.2 Реалізація апаратної частини пристрою	39
3.3 Тестування ефективності пристрою.....	43
3.4 Висновок до розділу 3.....	54
ВИСНОВКИ	55
ПЕРЕЛІК ПОСИЛАНЬ	56
Додаток А. Технічне завдання	60

Додаток Б. Лістинг програмного коду	64
Додаток В. Ілюстраційний матеріал	67

ВСТУП

Актуальність. У сучасному світі інформація є одним з найважливіших ресурсів, а забезпечення її конфіденційності, цілісності та доступності стає пріоритетним завданням як для державних та корпоративних структур, так і для приватних осіб. Особливої актуальності набуває захист мовної інформації, яка може бути перехоплена через акустичні канали спеціальними технічними засобами або ж випадковим підслуховуванням.

Однією з найбільш небезпечних загроз у сфері технічної розвідки є зйом інформації за допомогою мікрофонів направленої дії. Такі пристрої здатні вловлювати мовні сигнали навіть на значних відстанях через огорожувальні конструкції, що є серйозними ризиками для витоку конфіденційних даних. Ситуація ускладнюється тим, що засоби акустичного шпигунства постійно вдосконалюються, їх розміри зменшуються, а у чутливість зростає.

У відповідь на зростання рівня загрози, з'являється потреба у створенні спеціалізованих пристроїв, що здатні забезпечити активний захист від перехоплення інформації через акустичний канал. Одним із найефективніших методів є створення акустичних завад за допомогою шуму у мовному діапазоні, що суттєво ускладнює або унеможливорює перехоплення мови мікрофоном.

Метою даної роботи є розробка та виготовлення пристрою для захисту інформації від зйому мікрофоном направленої дії шляхом створення спрямованої шумової завади у заданому частотному діапазоні.

Для досягнення мети необхідно вирішити такі задачі:

- провести аналіз загроз, пов'язаних із перехопленням інформації через акустичний канал;
- вивчити принципи роботи мікрофонів направленої дії та методи боротьби з ними;
- проаналізувати існуючі пристрої та технології активного акустичного маскування;
- обґрунтувати вибір принципу дії, елементної бази та технічних параметрів

пристрою;

- розробити алгоритм генерації шуму та схемне рішення;
- реалізувати прототип пристрою та перевірити його ефективність

експериментально.

Об’єктом дослідження є технічні канали витоку мовної інформації внаслідок її зйому мікрофонами направленої дії.

Предметом дослідження є методи та засоби створення акустичних завад у мовному діапазоні для протидії акустичному шпигунству.

Новизна роботи полягає у розробці мобільного та адаптивного пристрою активного захисту, що реалізує принцип маскування мовної інформації шляхом генерацією шуму з випадковою частотною модуляцією, що підвищує ефективність його використання проти спрямованих мікрофонів.

Практична цінність полягає у можливості застосування пристрою в переговорних кімнатах, службових кабінетах, залах засідань та інших приміщеннях, де необхідно забезпечити високий рівень конфіденційності мовлення.

1 ЗАГАЛЬНИЙ АНАЛІЗ СИСТЕМ ЗАХИСТУ ВІД АКУСТИЧНОГО ЗЙОМУ ІНФОРМАЦІЇ

У цьому розділі здійснюється аналіз існуючих систем захисту інформації від витоку через акустичний канал, зокрема за допомогою мікрофонів направленої дії, закладних пристроїв, а також через випадкове перехоплення звукових коливань у середовищі. Розглядаються основні поняття, принципи функціонування каналів витоку, типові засоби акустичної розвідки, а також методи активного та пасивного захисту. Особливу увагу приділено характеристикам спрямованих мікрофонів як загрози для конфіденційності мовної інформації, після чого буде сформовано висновок та здійснено постановку задачі.

1.1 Основні поняття та загрози зйому інформації акустичним каналом

Акустичний канал витоку інформації – це фізичний шлях поширення звукових коливань від джерела (наприклад, голосу людини) до засобу їх перехоплення, зазвичай – мікрофона або іншого чутливого пристрою. З технічної точки зору, такий канал може виникати у повітряному середовищі, крізь щілини, вентиляційні отвори, а також стіни чи інженерні комунікації. Це зумовлено здатністю звукових хвиль поширюватись як в повітрі, так і через тверді поверхні що створює можливість перехоплення інформації.

Звук поширюється у вигляді механічних коливань частинок середовища, зокрема повітря, рідин або твердих тіл. У повітрі ці коливання передаються у вигляді поздовжніх хвиль, що змінюють тиск у середовищі. У твердих тілах виникають віброакустичні коливання, що можуть бути джерелом витоку навіть при відсутності прямого контакту з приміщенням, у якому озвучується інформація [1].

Акустичний канал витоку інформації виникає тоді, коли ці звукові хвилі досягають конструктивних елементів приміщення (скло, стіни, двері), змушують їх коливатись, а ті, у свою чергу, випромінюють звукову або віброакустичну енергію за межі контрольованої зони. За межами приміщення ці коливання можуть бути

вловлені різними пристроями, включно зі спрямованими мікрофонами, електронними стетоскопами, лазерно-оптичними системами та радіозакладками.

Найбільш поширеними загрозами є:

- перехоплення мовної інформації за допомогою мікрофонів направленої дії, встановлених на відстані;
- використання закладних пристроїв, приховано розміщених у приміщенні або на прилеглих територіях;
- випадкове поширення звуку через конструктивні особливості будівель, вентиляційні канали, електромережу або інші неекрановані інфраструктурні елементи.

Особливої уваги потребує так званий "мембранний ефект", коли звукова хвиля змушує тонкі й гнучкі елементи (віконне скло, гіпсокартон, пластикові перегородки) коливатися, тим самим утворюючи канал витоку. Аналогічно небезпечними є мікроскопічні щілини або отвори у конструкціях, через які звук безперешкодно проникає назовні [2].

Таким чином, загрози зйому інформації акустичним каналом охоплюють широкий спектр методів технічної розвідки, що потребують комплексного та продуманого підходу до організації захисту. Надійне протистояння таким загрозам можливе лише шляхом поєднання технічних засобів, архітектурних рішень і активних шумових систем маскування.

1.2 Технічні засоби перехоплення інформації через акустичний канал

Сучасні засоби технічної розвідки дозволяють здійснювати перехоплення мовної інформації без фізичного доступу до об'єкта озвучення. Акустичні канали витоку активно використовуються для здійснення несанкціонованого зйому за допомогою спеціалізованих пристроїв, що різняться за принципом дії, рівнем маскування та способом передавання інформації.

Серед найбільш поширених типів пристроїв, що застосовуються для перехоплення звукової інформації, можна виділити такі:

– мікрофони направленої дії – це пристрої з вузьким кутом сприйняття, які здатні вловлювати мовлення з великої відстані. Завдяки фокусуванню звукових хвиль, вони дозволяють перехоплювати розмови навіть через зачинені вікна або з відкритої місцевості. Прикладом є Sennheiser MKE 600 – мікрофон типу «шотган» (рис. 1.1) з суперкардіоїдною діаграмою спрямованості. Принцип дії такого мікрофона базується на фокусуванні звукових хвиль у вузькому напрямку за допомогою: довгої акустичної трубки, що діє як хвильовід і приглушує бокові звуки, або параболічного рефлектора, який концентрує звукові коливання в одній точці, де встановлений мікрофонний елемент.

Зібраний звуковий сигнал далі обробляється підсилювачем і передається або на запис, або бездротово до приймача зловмисника.



Рисунок 1.1 – Мікрофон направленої Sennheiser MKE 600

На рисунку 1.2 представлено загальну схему роботи мікрофона направленої дії в умовах перехоплення інформації через скло.

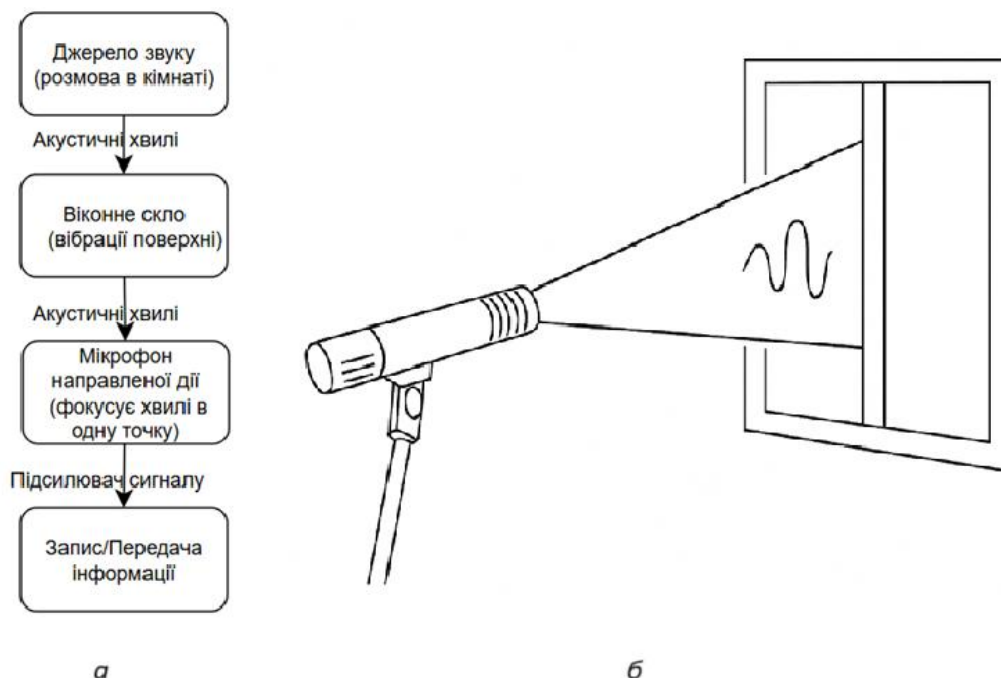


Рисунок 1.2 – Мікрофон направленої а) схема роботи б) ілюстрація роботи

– електронні стетоскопи – пристрої, які вловлюють вібрації конструкцій (стіни, труби, перекриття) й дозволяють прослуховувати розмови через тверді поверхні. Особливо ефективні в умовах, коли акустичний канал проходить через пружне середовище (рис. 1.3);



Рисунок 1.3 – Електронний стетоскоп Sun-Mechatronics MW-25

– радіозакладки – мініатюрні передавачі, які монтуються у приміщенні, меблях або електроніці. Зібрану інформацію вони передають через радіоканал на приймач зловмисника (рис. 1.4);



Рисунок 1.4 – Радіозакладка RMK-129

– диктофони та замасковані рекордери – портативні пристрої для запису, які часто маскуються під повсякденні предмети: ручки, флешки, годинники, брелоки тощо. Використовуються для короткотермінового доступу до об'єкта (рис. 1.5);



Рисунок 1.5 – Замаскований диктофон MemoQ MQ-78 Pen

– лазерно-оптичні системи зйому – високоточні пристрої, що використовують лазерний промінь для фіксації мікрівібрацій об'єктів (наприклад, віконного скла), які виникають під впливом звукової хвилі зсередини приміщення (рис. 1.6).



Рисунок 1.6 – Лазерний мікрофон GMD2200NEO

Порівняльні характеристики розглянутих засобів акустичного зйому наведено в таблиці 1.1.

Таблиця 1.1 – Порівняльна характеристика існуючих аналогів

Назва пристрою	Дальність дії	Тип передачі даних	Основна сфера застосування
Sennheiser MKE 600 [3]	до 50 м	дротовий аудіовихід	Відеозйомка, документалістика, польові записи
Sun-Mechatronics MW-25 [4]	через стіни (до 30 см)	дротовий аудіовихід	прослуховування через тверді конструкції
RMK-129 [5]	до 1 км	аналоговий радіосигнал (UHF)	приховане прослуховування в приміщенні
MemoQ MQ-78 Pen [6]	до 15 м	внутрішня пам'ять	замаскований запис під виглядом повсякденного предмета
GMD2200NEO [7]	до 300 м	оптичний канал	дистанційне прослуховування через віконне скло

Як видно з таблиці 1.1, пристрої для зйому акустичної інформації мають суттєві відмінності за дальністю дії, типом передачі сигналу та сферою застосування. Наприклад, Sennheiser MKE 600 дозволяє здійснювати зйом мовлення на відстані до 50 метрів, що робить його ефективним у відкритому просторі або при наявності прямої звукової видимості. Водночас, лазерний мікрофон GMD2200NEO здатний

зчитувати мікровібрації на відстані до 300 м, при цьому передаючи інформацію через оптичний канал, що забезпечує високу скритність.

Закладка RMK-129 має найбільшу дальність – до 1 км – завдяки радіоканалу UHF, але потребує попередньої установки у приміщенні. Sun-Mechatronics MW-25 працює безпосередньо через стіну (до 30 см товщиною), що робить його ефективним для перехоплення через будівельні конструкції. При цьому МетоQ MQ-78 Pen є прикладом пристрою ближнього доступу (до 15 м), замаскованого під звичайний предмет, що дозволяє використовувати його без підозр.

Таким чином, технічні засоби перехоплення покривають усі варіанти дистанційного перехоплення від ближніх до далеких і вимагають комплексного підходу до захисту, особливо в приміщеннях із потенційним витоком інформації.

1.3 Дослідження існуючих технічних рішень

Основна ідея захисту інформації від витоків через акустичний канал полягає у порушенні передачі звукової інформації від джерела до засобу перехоплення. У загальному випадку ефективність захисту мовної інформації оцінюється за допомогою співвідношення сигнал/завада:

$$SNR = 10 \log \frac{P_{\text{сиг}}}{P_{\text{зав}}}$$

де: $P_{\text{сигнал}}$ – потужність корисного сигналу (мови); $P_{\text{зав}}$ – потужність завади, яка накладається на сигнал.

Для ефективного захисту необхідно забезпечити умову:

$$SNR < P_{\text{мін. допустиме}}$$

Іншими словами необхідно створити достатній рівень завади задля спотворення мовної інформації настільки, що вона стане непридатною для відновлення [8]. Це можна реалізувати двома способами: підвищити рівень завад і в результаті інформацію буде неможливо виокремити або знизити рівень корисного сигналу настільки, що його буде неможливо вловити. У першому випадку реалізуються активні методи, які передбачають створення додаткового шумового фону або вібраційних завад у необхідному діапазоні. У другому випадку застосовуються

пасивні методи, що фізично обмежують поширення звукових хвиль, такі як: звукоізоляція, екранування, герметизація приміщень тощо. Саме на активному підході ґрунтується більшість сучасних систем акустичного маскуванню.

Найбільш поширені технічні засоби захисту від акустичного зйому включають:

- акустичне маскуванню в мовному діапазоні – генерація білого або рожевого шуму в межах 300–4000 Гц, що перекриває спектр людського мовлення та унеможлиблює його розпізнавання засобами перехоплення;

- акустичне маскуванню у високочастотному діапазоні – створення шумових завад вище мовного спектру з метою перешкоджання роботі пристроїв, чутливих до вищих гармонік або для маскуванню ультразвукових каналів;

- віброзахист – передача шуму у тверді конструкції (стіни, вікна) за допомогою спеціальних віброгенераторів, що спричиняють коливання поверхні та перешкоджають перехопленню через конструктивні елементи;

- комбіновані системи – поєднання в одному рішенні акустичного та вібраційного маскуванню для розширеного покриття загроз;

- пасивне екранування – використання спеціалізованих матеріалів для зменшення поширення звуку. До таких рішень належать акустичні панелі, звукопоглинальні штори, подвійні стіни, тощо.

Засоби захисту інформації від зйому через акустичний канал широко застосовуються в приміщеннях, де виникає необхідність у забезпеченні конфіденційності переговорів або виключенні можливості технічного прослуховування. Типовими прикладами таких об'єктів є:

- конференц-зали в органах державної влади, зокрема під час нарад із доступом до службової або таємної інформації;

- адвокатські офіси та приміщення нотаріусів, де здійснюється обробка персональних даних та інформації, що охороняється законом;

- переговорні кімнати підприємств, особливо в умовах комерційної таємниці або обговорення стратегічних рішень;

- ситуаційні центри, штаби, командні пункти у структурах оборони, безпеки або надзвичайного реагування;

– приміщення керівного складу компаній, банків, ІТ-компаній тощо.

Залежно від архітектури приміщення, рівня загрози та наявних каналів витоку, можуть застосовуватись різні комбінації активного та пасивного захисту. Зокрема, у великих залах часто поєднують віброакустичні засоби з акустичним маскуванням та локальним екрануванням.

Опис деяких приладів маскування наведено в таблиці 1.2.

Таблиця 1.2 – Характеристики пристроїв захисту від акустичного зйому

Тип захисту	Назва пристрою	Енергоживлення	Метод захисту	Захист
Акустичне (мовне)	DNG-2300	10 Вт	Генерація білого шуму	Спрямовані мікрофони, диктофони
Акустичне (високе)	NG-220	12 Вт	Генерація широкосмугового шуму	Лазерні мікрофони, ультразвукові системи
Віброзахист	ВЗГ-3	15 Вт	П'єзовібратор для стін/скла	Електронні стетоскопи, віброзйом
Комбінований	Барс + ВЗГ-3 (система)	25 Вт	Акустичне та віброакустичне маскування	Мікрофони, закладки, лазерні мікрофони
Пасивний	Zaslon	Не потребує	Звукопоглинальний екран	Загасання мовлення в межах перегородки

Виходячи з даних таблиці 1.2, можна зробити такі висновки щодо ефективності та обмежень розглянутих пристроїв:

DNG-2300 є генератором білого шуму з енергоспоживанням 10 Вт і радіусом дії до 5 м. Пристрій забезпечує ефективне акустичне маскування мовної інформації у невеликих приміщеннях, зокрема в переговорних кімнатах. Основним недоліком є обмежена зона покриття та відсутність дії на віброакустичні канали витоку [9].

NG-220 створює широкосмугові завади у високочастотному діапазоні, споживає 12 Вт та охоплює зону до 6 м. Ефективно протидіє лазерним мікрофонам і ультразвуковим системам, проте не забезпечує належного маскування в мовному діапазоні, що унеможлиблює його застосування проти традиційних мікрофонів направленої дії [9].

ВЗГ-3 реалізує віброакустичний принцип захисту з передачею шумових сигналів у тверді конструкції. При потужності 15 Вт і покритті до 4 м пристрій ефективний у нейтралізації електронних стетоскопів. Водночас він не створює

повітряних акустичних завад, що обмежує його застосування в умовах відкритих каналів витоку [9].

Барс + ВЗГ-3 є комбінованою системою, що поєднує акустичне та віброакустичне маскування. При загальному енергоспоживанні 25 Вт забезпечується захист у межах до 6 м, що робить цю систему однією з найефективніших серед розглянутих. До основних обмежень належать висока вартість, потреба в монтажі та відносно велике енергоспоживання [9].

Zaslon – пасивний засіб захисту, який не потребує електроживлення та реалізує звукопоглинання шляхом фізичного послаблення звукових хвиль. Однак відсутність активної дії, нездатність протидіяти направленим каналам витоку або вібраціям обмежує ефективність засобу у випадках наявності технічного перехоплення [9].

Проведене порівняння дозволяє зробити висновок, що активні засоби захисту є більш універсальними та гнучкими в умовах реального часу, особливо при цілеспрямованій дії на мовний або віброакустичний діапазон. Натомість пасивні рішення не можуть забезпечити повноцінного рівня захисту за відсутності додаткових активних компонентів.

Для забезпечення комплексної безпеки мовної інформації доцільним є використання комбінованого підходу, що включає як активні, так і пасивні засоби захисту. Такий підхід повинен базуватися на аналізі потенційних каналів витоку та специфіці приміщення, в якому забезпечується захист.

1.4 Мікрофони направленої дії: принцип роботи, чутливість та недоліки

Мікрофони направленої дії є одним із найбільш поширених і ефективних засобів зйому акустичної інформації на відстані. Через їх спеціальну конструкцію та принцип роботи, що орієнтований на вибіркове захоплення звукових коливань в певному напрямку, а також максимальному приглушенні шумів що знаходяться із боків та тилу.

Основою таких пристроїв є спрямований акустичний канал, що досягається за рахунок:

- використання акустичних трубок, що працюють як хвильоводи;
- застосування параболічного дзеркала, яке фокусує звукові хвилі з великої площі в одну точку, де розміщується мікрофонний елемент;
- комбінації електронної обробки сигналів (цифрових фільтрів, фазових компенсацій), які посилюють сигнали із заданого напрямку та приглушують інші.

За рахунок цього досягається вузька діаграма спрямованості, яка дозволяє концентрувати чутливість мікрофона в межах кількох десятків кутових градусів, ігноруючи фонові шуми з інших боків [10].

Чутливість та характеристики мікрофонів направленої дії:

- коефіцієнт спрямованості: чутливість по осі в вища, ніж з боків;
- чутливість – від -45 дБ до -33 дБ (залежно від конструкції);
- робочий діапазон частот – $100\text{--}16000$ Гц;
- ефективна дальність захоплення мовлення – від 10 до 200 метрів (для параболічних моделей – більше).

Наприклад, мікрофон Sennheiser MKE 600 належить до категорії спрямованих мікрофонів типу «шотган» з суперкардіоїдною діаграмою спрямованості та здатен ефективно вловлювати мовлення на дистанції до 50 метрів за умови низького рівня фонового шуму.

Попри високу ефективність у перехопленні мовної інформації, мікрофони направленої дії мають низку обмежень, які слід враховувати. По-перше, висока залежність від точного спрямування – навіть незначне відхилення осі мікрофона від джерела звуку призводить до суттєвого зниження чутливості та якості запису. По-друге, обов'язкова наявність прямої звукової видимості – при наявності фізичних перешкод (стіни, подвійне скло, масивні штори) ефективність мікрофона різко зменшується або стає нульовою. По-третє, чутливість до зовнішніх чинників – погодні умови (дощ, вітер), сторонні шуми, реверберація або акустичне перевідбиття у приміщеннях можуть викривлювати або погіршувати сигнал. По-четверте, значне зменшення ефективної дальності в реальних умовах – якщо в лабораторних умовах мікрофон може вловлювати розмову на $100\text{--}200$ м, то в міському середовищі ця дистанція скорочується в кілька разів. По-п'яте,

вразливість до активних завад – навіть простий генератор білого чи рожевого шуму здатен ефективно блокувати спроби перехоплення шляхом маскуванню мовного сигналу.

Через високу ефективність та відносну доступність мікрофони направленої дії становлять реальну загрозу витоку мовної інформації, особливо в умовах недостатнього акустичного захисту приміщень. У той же час їх ефективність значною мірою обмежується зовнішніми чинниками – наявністю перешкод, активних шумових завад або конструктивної звукоізоляції. Саме тому при побудові систем технічного захисту інформації необхідно ретельно враховувати як потенційні можливості таких пристроїв, так і умови, що знижують їхню ефективність.

1.5 Висновки до розділу 1 та постановка задачі

У результаті проведеного аналізу встановлено, що акустичний канал є одним із найбільш уразливих шляхів витоку мовної інформації, оскільки дозволяє передавати звукові коливання не лише через повітряне середовище, але й через тверді конструкції приміщення. Це створює можливості для несанкціонованого зйому інформації за допомогою технічних засобів, які не потребують фізичного доступу до захищеної зони. Розглянуті технічні засоби перехоплення, зокрема спрямовані мікрофони, електронні стетоскопи, лазерні мікрофони, закладки та замасковані диктофони, демонструють різні підходи до зйому інформації та суттєво відрізняються за принципом дії, дальністю, способом передачі даних і рівнем замаскованості.

Окрему увагу було приділено мікрофонам направленої дії як одному з найнебезпечніших інструментів перехоплення мовної інформації. Попри їхню високу ефективність, вони мають обмеження, пов'язані з необхідністю точного спрямування, наявністю прямої звукової видимості та високою вразливістю до акустичних завад. Це відкриває можливості для ефективного технічного протидіяння за умови правильного вибору підходу до захисту.

На основі проведеного аналізу сформовано задачі подальшої роботи, зокрема визначення оптимального принципу дії, вибір відповідної елементної бази, розробка алгоритму створення акустичних завад та експериментальна перевірка ефективності створеного пристрою в умовах потенційного зйому інформації.

2 РОЗРОБКА ПРИСТРОЮ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ЗЙОМУ МІКРОФОНОМ НАПРАВЛЕНОЇ ДІЇ

У цьому розділі розглянуто практичні аспекти побудови пристрою, призначеного для захисту мовної інформації від зйому мікрофонами направленої дії шляхом створення активних акустичних завад. На основі проведеного аналізу та обґрунтованого вибору технічного підходу сформовано вимоги до функціональності пристрою, підібрано відповідну елементну базу та запропоновано архітектурну схему реалізації.

Описано логіку роботи системи, принцип формування шуму, особливості підключення компонентів, а також обрані програмні засоби та мову розробки. Результатом цього етапу є створення проєктної основи пристрою, придатної для подальшої реалізації, налаштування та тестування в умовах, наближених до реального застосування.

2.1 Обґрунтування вибору технічного підходу

Як було проаналізовано у розділі 1, одним із найефективніших методів протидії несанкціонованому зняттю акустичної інформації, зокрема мікрофонами направленої дії, є генерація акустичних завад. Цей підхід знижує співвідношення сигнал/завада (SNR) у напрямку потенційного перехоплення, що ускладнює або унеможливорює розбірливе відтворення мовної інформації.

На відміну від пасивних методів, таких як звукоізоляція або екранування, активне маскування не потребує складного монтажу чи втручання в конструкцію приміщення. Його перевагами є:

- мобільність, пристрій легко розгортається у будь-якому приміщенні без необхідності структурних змін;
- низьке енергоспоживання, що забезпечує тривалу автономну роботу;
- простота налаштування, пристрій не потребує складного конфігурування для ефективного функціонування. [11].

Однак слід враховувати обмеження:

– неефективність проти вібраційного зняття: акустичне маскування не захищає від перехоплення через конструктивні елементи, які передають вібрації краще, ніж повітря (наприклад, через стіни чи труби);

– можливий дискомфорт: надмірна гучність завад може викликати дискомфорт у присутніх.

З урахуванням технічної реалізованості та ефективності захисту, в рамках цієї роботи було обрано варіант створення пристрою, що генерує акустичні завади в діапазоні 300–3400 Гц. Саме цей діапазон є найбільш чутливим для мікрофонів направленої дії та охоплює основну частину спектру людської мови.

Для генерації завад доцільно використовувати псевдовипадковий білий або рожевий шум. Псевдовипадковим називається такий сигнал, що виглядає випадковим, але генерується за детермінованим алгоритмом. Білий шум має рівномірний спектр потужності на всіх частотах, що робить його ефективним для маскування широкого діапазону сигналів. Рожевий шум характеризується зниженням енергії зі зростанням частоти (залежність обернено пропорційна до частоти), він сприймається більш природно для слуху людини та часто використовується в акустичному маскуванні в приміщеннях [12].

З технічної точки зору, створення такого шуму може бути реалізоване на основі мікроконтролера з програмним генератором псевдовипадкових послідовностей. Сформований сигнал через цифро-аналоговий перетворювач (ЦАП) подається на динамік, який випромінює акустичну заваду у навколишнє середовище в межах заданого простору. У випадку мікрофонів направленої дії, які є основною загрозою в рамках цієї роботи, активне акустичне маскування демонструє високу ефективність. Це зумовлено тим, що спрямованість мікрофона значно підвищує його чутливість до фронтального шуму, який перебиває мовний сигнал. Для узагальнення ефективності активного маскування щодо різних типів мікрофонів (включно з направленими), у таблиці 2.1 наведено порівняльні дані.

Таблиця 2.1 – Ефективність активного акустичного маскування залежно від типу мікрофона

Тип мікрофона	Чутливість до маскування	Коментар
Направлений (кардіоїдний)	Висока	Ефективно блокується фронтальним шумом у мовному діапазоні
Суперкардіоїдний / гіперкардіоїдний	Середня	Менш вразливі збоку, але все ще блокуються фронтальним шумом
Омнідирекційний	Низька	Уловлює звук з усіх напрямків – потрібна більша потужність шуму
Мікрофонний масив (Beamforming)	Висока	Залежить від алгоритму, але маскування спектра ускладнює обробку
Прикордонний (boundary mic)	Середня	Потребує шуму, що спрямований по площині розміщення

Як показано в таблиці 2.1, активне акустичне маскування є особливо ефективним проти мікрофонів направленої дії, що підтверджує обґрунтованість обраного технічного підходу. Це дозволяє з високою ймовірністю знизити якість перехопленого сигналу до рівня, непридатного для розпізнавання мовної інформації.

У порівнянні з іншими типами мікрофонів, спрямовані пристрої найбільш чутливі до фронтального шуму, що дає змогу забезпечити надійний захист навіть у простих умовах. Водночас у випадку омнінаправлених або лазерно-оптичних мікрофонів можуть знадобитися додаткові заходи захисту – зокрема, віброакустичні або широкосмугові завади.

Загалом, вибраний підхід поєднує простоту реалізації, гнучкість налаштувань, ефективність у реальному середовищі та можливість автономної роботи. Завдяки використанню програмованого мікроконтролера, створюється мобільний пристрій, здатний забезпечити цілеспрямоване маскування мовної інформації в критичних зонах безпеки.

2.2 Обґрунтування вибору елементної бази

Під час проєктування пристрою активного акустичного маскування було здійснено вибір елементної бази, яка забезпечує необхідну функціональність при мінімальних витратах, збереженні компактності та простоти реалізації. Основними критеріями стали здатність системи генерувати акустичні завади у мовному діапазоні, надійна робота в автономному режимі та стабільність при живленні від стандартних джерел постійної напруги.

На етапі концептуального вибору було відмовлено від використання апаратних джерел шуму – таких як стабілітрони, транзистори в режимі шумогенерації або спеціалізовані мікросхеми. Основними причинами стали обмеженість спектру та складність точного контролю частотних характеристик у таких рішеннях. Крім того, апаратні генератори потребують додаткових аналогових схем для підсилення та фільтрації, що ускладнює конструкцію, підвищує енергоспоживання та знижує масштабованість системи.

Причини відмови від апаратного генератора шуму:

- обмежений контроль над спектром;
- відсутність можливості перемикання між режимами;
- неможливість інтеграції з ботами або розумним керуванням;
- відсутність адаптації під змінні умови.

Натомість було обрано програмно-цифровий підхід із використанням мікроконтролера ESP32 та внутрішніх DAC, що дасть змогу:

- створювати як білий, так і рожевий шум із різними параметрами в реальному часі;
- швидко перемикати режими без зміни апаратної конфігурації;
- реалізувати дистанційне керування через Telegram-інтерфейс;
- забезпечити гнучкість для подальшого вдосконалення програмного забезпечення;
- зменшити габарити, вартість і загальну складність пристрою.

Центральним керуючим компонентом обрано мікроконтролер ESP32 DevKit V1, (рис. 2.1) оснащений двоядерним процесором Tensilica LX6 із тактовою частотою до 240 МГц та 520 КБ оперативної пам'яті, що забезпечує достатній обчислювальний ресурс для генерації псевдовипадкових шумових сигналів у режимі реального часу (див. табл. 2.2) [13].



Рисунок 2.1 – Мікроконтролер ESP32 DevKit V1

Для оцінки доцільності вибору ESP32 DevKit V1 як центрального елемента системи було проведено порівняння його ключових характеристик із популярною платформою Arduino Uno R3, яка часто використовується в базових проєктах з генерацією сигналів та керуванням пристроями. Наведена таблиця демонструє переваги ESP32 у контексті створення пристрою активного акустичного маскування:

Таблиця 2.2 – Основні характеристики Esp32 DevKit v1 та Arduino Uno R3

Характеристика	ESP32 DevKit V1	Arduino Uno R3
Процесор	Xtensa LX6, 32-bit, 1/2 ядра	ATmega328P, 8-bit
Тактова частота	до 240 МГц	16 МГц
ОЗП (SRAM)	520 КБ	2 КБ
Постійна пам'ять (Flash)	4 МБ	32 КБ
Аналогові входи (ADC)	6	6
Аналогові виходи (DAC)	2 (вбудовані)	відсутні (лише ШІМ)
Цифрові входи/виходи (GPIO)	25	14
Підтримка Wi-Fi / Bluetooth	вбудовані	відсутні (необхідні додаткові модулі)

Продовження таблиці 2.2

Живлення	5 В (через USB) / VIN 7–12 В	5 В (через USB) / VIN 7–12 В
Програмування	Arduino IDE, ESP-IDF	Arduino IDE
DAC-вивід для звуку	так (вбудовано)	ні (потрібен зовнішній ЦАП)
Дистанційне керування (боти)	можливе без додаткового обладнання	лише з додатковими модулями

На основі порівняння можна зробити висновок, що ESP32 DevKit V1 значно переважає Arduino Uno R3 за обчислювальною потужністю, обсягами пам'яті, наявністю вбудованих засобів бездротового зв'язку та можливістю генерації аналогових сигналів. Ці параметри є критично важливими для реалізації ефективного та компактного пристрою акустичного маскуванню, здатного працювати автономно та взаємодіяти з користувачем через мобільний інтерфейс. Вибір ESP32 дозволив обійтись без зовнішніх модулів, зменшити складність схеми та підвищити функціональність системи в цілому.

Для підсилення сигналу, сформованого ESP32, використовується аудіопідсилювач PAM8403, що є двоканальним підсилювачем класу D. Завдяки архітектурі класу D, PAM8403 забезпечує високу енергоефективність (до 90 %) при компактному розмірі та мінімальному тепловиділенні. Це особливо актуально для автономних пристроїв, які працюють від акумулятора, адже дає змогу тривалий час підтримувати гучність без перегріву.

PAM8403 працює при напрузі живлення 5 В, що дозволяє використовувати його спільно з мікроконтролером ESP32 без необхідності додаткових стабілізаторів. При навантаженні 4 Ом підсилювач може забезпечити до 3 Вт на канал, чого цілком достатньо для досягнення помітного ефекту акустичного зашумлення в невеликих приміщеннях (до 20 м²).

Крім того, модуль підтримує вихід у мостовому режимі (BTL), що дає змогу отримати більшу потужність без зовнішніх компонентів. Наявність вбудованого захисту від короткого замикання, перегріву та перенапруги також робить PAM8403 надійним рішенням для вбудованих пристроїв. (рис. 2.2).



Рисунок 2.2 – Підсилювач РАМ8403

У контексті реалізації компактного пристрою акустичного зашумлення РАМ8403 є оптимальним вибором завдяки:

- сумісності з ESP32 по напрузі живлення;
- достатній вихідній потужності для невеликих приміщень;
- компактним габаритам і простоті інтеграції;
- низькому енергоспоживанню, що важливо для живлення від power bank.

Живлення подається безпосередньо від USB або порту VIN ESP32 (5 В), що одночасно забезпечує живлення для ESP32 та РАМ8403, зберігаючи простоту конструкції.

Для відтворення шуму застосовуються динаміки з опором 8 Ом та потужністю 2 Вт, що є оптимальними для даної конфігурації. Вони дозволяють охопити простір у радіусі до 2–3 метрів із рівнем шуму, достатнім для маскування мовлення у приміщенні невеликого або середнього розміру. Конструктивно динаміки можуть бути виконані у формі класичних динамічних випромінювачів або плоских резонаторів, залежно від вимог до монтажу, спрямованості та акустичного оформлення (рис. 2.3).

Звуковий тиск, створюваний динаміками, прямо залежить від їхньої потужності та ефективності підсилювача. У даному випадку використання компактного підсилювача РАМ8403 дозволяє максимально розкрити потенціал динаміків при мінімальному споживанні енергії. Наявність двох окремих каналів дає змогу реалізувати як односпрямоване звучання, так і просторове (стерео або зональне) маскування. Важливим критерієм вибору динаміків стало також їхнє

співвідношення розмірів до гучності, що дозволяє вбудовувати їх у компактні корпуси або маскувати в елементах інтер'єру.

У разі необхідності розширення зони покриття або підвищення ефективності захисту, динаміки можуть бути замінені на моделі більшої потужності або доповнені акустичними хвилеводами, що підсилюють направленість звуку в певному секторі.



Рисунок 2.3 – Приклад динаміків 8 Ом / 2 Вт для генерації шуму

Запропонована комбінація ESP32, PAM8403 та динаміків дозволяє реалізувати повноцінний пристрій акустичного захисту, який може ефективно функціонувати в умовах обмеженого простору без потреби в складному живленні чи додаткових модулях. Така конструкція є оптимальною за критеріями енергоефективності, вартості та простоти обслуговування.

2.3 Обґрунтування вибору мови програмування

З програмної точки зору розробка пристрою ведеться у середовищі Arduino IDE – популярній платформі з відкритим кодом, яка забезпечує зручний інтерфейс для роботи з мікроконтролерами, зокрема з ESP32. Arduino IDE підтримує велику кількість бібліотек для роботи з DAC, PWM, GPIO, UART, таймерами, а також надає вбудовані засоби компіляції, налагодження та завантаження прошивки у пристрій [16].

Проте, мікроконтролер ESP32 не підтримується в стандартній версії Arduino IDE, тож для повноцінної роботи з ним необхідно встановити додаткову платформу Espressif ESP32, що розширює функціонал середовища. Після встановлення цієї платформи користувач отримує доступ до повного набору функцій ESP32: робота з вбудованими DAC-виходами, Wi-Fi, Bluetooth, SPI, I²C, таймерами, FreeRTOS-задачами тощо.

Ця реалізація базується на бібліотеці esp32 від Espressif Systems – офіційного розробника мікросхеми. Бібліотека постійно оновлюється, має широкую документацію та активну спільноту, що дозволяє реалізовувати як базові, так і складні функції без потреби у низькорівневому програмуванні. Для ініціалізації DAC, організації Wi-Fi-з'єднання та взаємодії з Telegram-ботом використано бібліотеки WiFi.h, WiFiClientSecure.h, UniversalTelegramBot.h, а також ArduinoJson.h для обробки вхідних повідомлень [17].

У якості інтерфейсу дистанційного керування пристроєм застосовується Telegram-бот, реалізований з використанням бібліотеки UniversalTelegramBot. Бот функціонує через захищене з'єднання (HTTPS) і дозволяє користувачеві за допомогою текстових команд вмикати або вимикати генерацію шуму, а також обирати тип шуму (білий або рожевий). Такий спосіб керування є зручним, безпечним і не потребує додаткових додатків або фізичних інтерфейсів. Передбачена підтримка клавіатури із кнопками та реакція на вхідні команди у режимі реального часу [18].

Основною мовою програмування у середовищі Arduino є C++, яка дає змогу ефективно взаємодіяти з апаратними ресурсами мікроконтролера. На відміну від інтерпретованих або візуальних мов, C++ забезпечує прямий контроль над регістрами, таймерами, внутрішніми шинами, генераторами переривань, що критично важливо для точного керування DAC-портами та синхронізації генерації псевдовипадкового шуму [19].

Однією з причин вибору C++ є можливість максимального використання ресурсів мікроконтролера при мінімальному навантаженні на пам'ять. Це особливо актуально у вбудованих системах, де розмір оперативної пам'яті обмежени. C++

дозволяє оптимізувати обсяг прошивки, уникати зайвих викликів функцій та управляти ресурсами на низькому рівні, зокрема через роботу з покажчиками, статичною пам'яттю та inline-функціями.

Крім того, об'єктно-орієнтований підхід, який підтримується в C++, дозволяє структурувати проєкт на окремі модулі: генерацію шуму, керування підсиленням, роботу з живленням тощо. Це забезпечує гнучкість, зручність супроводу, тестування та масштабування функціоналу, зокрема в разі, якщо в майбутньому буде реалізовано зміну частотного діапазону шуму або додано сенсорний ввід.

Також C++ має широку базу відкритих бібліотек (наприклад, ArduinoRandom, Audio, ESP-DAC), які можуть бути використані для реалізації псевдовипадкової генерації, фільтрації, керування звуковим профілем. Наявність активної спільноти, форумів та прикладів дає змогу значно прискорити розробку, усунути помилки та використовувати перевірені підходи, що підвищує надійність пристрою [20].

Таким чином, комбінація Arduino IDE та мови програмування C++ є найбільш раціональним вибором для реалізації інтелектуального керування генерацією шуму, забезпечує доступ до всіх необхідних апаратних функцій мікроконтролера ESP32, та відповідає вимогам до продуктивності, масштабованості та підтримки.

2.4 Структурна схема пристрою та сценарій його використання

Розроблений пристрій призначений для активного маскування мовної інформації шляхом генерації акустичних завад у частотному діапазоні людського мовлення (приблизно 300–3400 Гц). Функціонування системи базується на взаємодії апаратних компонентів, що забезпечують формування, підсилення та трансляцію шумового сигналу у середовище, а також реалізують живлення та можливість автономної роботи.

Мікроконтролер ESP32 виконує роль центрального елемента, який формує шумовий масив (білий або рожевий шум) та виводить його на цифрово-аналоговий перетворювач (DAC). Сформований сигнал надходить на підсилювальний модуль РАМ8403, після чого транслюється через динаміки у простір, створюючи завади для потенційних засобів перехоплення. Живлення забезпечується від стандартного

джерела постійної напруги 5 В, зокрема Power Bank або акумуляторного блоку. Структурна схема функціонування пристрою наведена на рисунку 2.4.

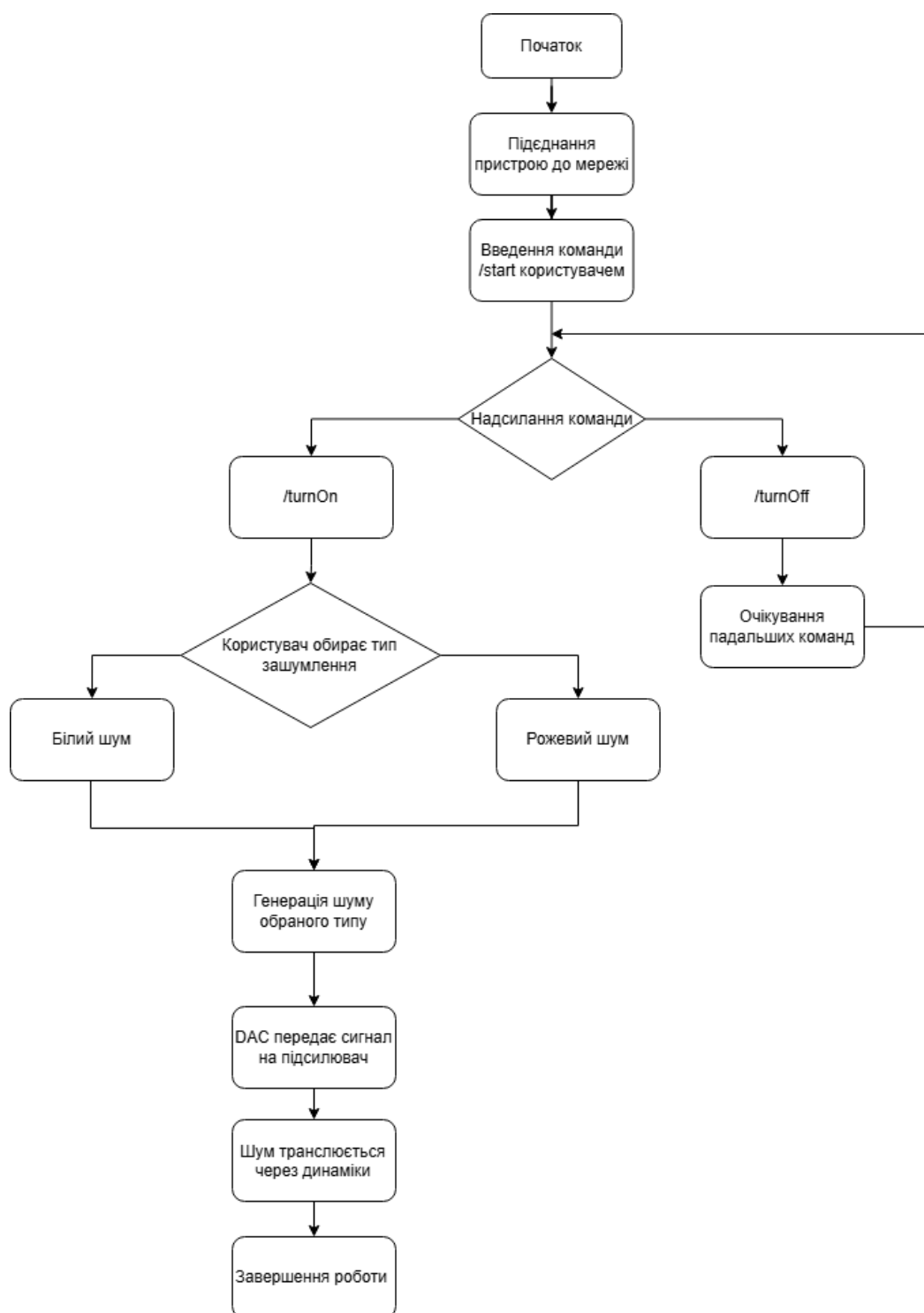


Рисунок 2.4 – Структурна схема роботи пристрою захисту мовної інформації

Як видно на рисунку робота пристрою реалізована відповідно до наступної послідовності дій:

Крок 1. ESP32 здійснює ініціалізацію системи та підключається до Wi-Fi-мережі з використанням попередньо збережених параметрів доступу.

Крок 2. Налагоджується захищене з'єднання з Telegram-ботом через API.

Крок 3. Telegram-бот переходить у режим очікування на вхідні команди від користувача.

Крок 4. Користувач надсилає одну з команд: /turnOn, /turnOff, /startWhite або /startPink.

Крок 5. У разі отримання команди активації, пристрій обирає відповідний тип шуму (білий або рожевий), що зберігається у вигляді масиву значень.

Крок 6. Шумовий масив передається на вихідні цифрово-аналогові перетворювачі (DAC) мікроконтролера.

Крок 7. Сигнал підсилюється модулем PAM8403 і транслюється через динаміки.

Крок 8. У режимі активного захисту система постійно оновлює шумовий сигнал та перевіряє надходження нових команд від користувача.

Крок 9. У разі отримання нової команди змінюється режим роботи або припиняється трансляція шуму.

Сценарії практичного використання пристрою охоплюють переговорні кімнати, службові кабінети, ситуаційні центри, приміщення для конфіденційних зустрічей. Пристрій може активуватись вручну, дистанційно або автоматично (у разі дооснащення таймером або датчиком присутності). Створюване шумове поле знижує ймовірність якісного перехоплення мовної інформації навіть за умови використання мікрофонів направленої дії або прихованих записуючих пристроїв.

За потреби можливе розширення функціоналу пристрою: збільшення кількості динаміків, розширення площі дії, реалізація адаптивного регулювання шуму залежно від рівня фонового звуку.

2.5 Висновки до розділу 2

У цьому розділі було здійснено обґрунтування вибору технічного підходу до побудови пристрою захисту інформації від зйому акустичним каналом. Визначено,

що найбільш доцільним методом у даному випадку є активне акустичне маскування шляхом генерації шумових завад у мовному діапазоні частот, що дозволяє ефективно протидіяти мікрофонам направленої дії та іншим засобам перехоплення.

Проведено обґрунтування вибору основних апаратних компонентів: мікроконтролера ESP32, підсилювального модуля PAM8403 та широкосмугових динаміків з опором 8 Ом і потужністю 2 Вт. Обрані елементи забезпечують компактність, енергоефективність, простоту реалізації та можливість автономної роботи пристрою.

Наведено структурну схему функціонування пристрою та описано його принцип роботи. Окрему увагу приділено середовищу програмування Arduino IDE та використанню мови програмування C++ як найбільш придатної для реалізації алгоритмів генерації шуму та керування компонентами.

У підсумку, у розділі сформовано повну концепцію апаратно-програмної реалізації пристрою активного акустичного захисту, що лягає в основу його практичної реалізації, описаної в наступному розділі.

3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПРИСТРОЮ АКТИВНОГО АКУСТИЧНОГО ЗАХИСТУ

В даному розділі наведено реалізацію апаратної та програмної частини пристрою захисту акустичної інформації від витоків шляхом використання мікрофона направленої дії. Детально описана логіка роботи, використані алгоритми та команди керування, реалізацію Telegram-інтерфейсу та створення шумових сигналів.

Здійснено опис апаратної реалізації пристрою і способів підключення компонентів. Також увагу приділено процедурі експериментального тестування ефективності генерації завад, яка дозволяє оцінити практичну придатність пристрою до використання у реальних умовах.

За результатами реалізації зроблено висновки щодо функціональності, стабільності та потенціалу використання системи.

3.1 Реалізація програмного забезпечення пристрою

Програмне забезпечення пристрою активного акустичного маскування реалізовано на мікроконтролері ESP32 DevKit V1 у середовищі Arduino IDE з використанням мови програмування C++. Програмна логіка охоплює підключення до Wi-Fi, взаємодію з Telegram API, генерацію шумових сигналів (білий або рожевий шум) та передавання сформованого сигналу на цифрово-аналогові виходи (DAC).

Ініціалізація мережі та підключення до Telegram-бота.

На етапі запуску пристрою здійснюється підключення до заданої Wi-Fi мережі та встановлюється зв'язок із Telegram-ботом. Для цього імпортуються відповідні бібліотеки та оголошуються параметри підключення:

```
#include <WiFi.h>
#include <WiFiClientSecure.h>
#include <UniversalTelegramBot.h>
const char* ssid = "*****";
const char* password = "*****";
```

```

#define BOT_TOKEN "*****"

WiFiClientSecure client;

UniversalTelegramBot bot(BOT_TOKEN, client);

void connectWiFi() {
    WiFi.begin(ssid, password);
    while (WiFi.status() != WL_CONNECTED) {
        delay(500);
    }
    client.setInsecure(); // Без перевірки сертифіката
}

```

Цей код забезпечує підключення до бездротової мережі та ініціалізацію клієнта Telegram через захищене з'єднання.

Генерація шуму.

Після ініціалізації система створює два масиви значень – білий шум та рожевий шум – які надалі використовуються для виводу сигналу через DAC-порти:

```

void generateWhiteNoise(uint8_t* pattern) {
    for (int i = 0; i < noiseLength; i++) {
        int base = random(100, 220);
        int modulation = random(-30, 30);
        pattern[i] = constrain(base + modulation, 0, 255);
    }
}

void generatePinkNoise(uint8_t* pattern) {
    float b0 = 0, b1 = 0, b2 = 0;
    for (int i = 0; i < noiseLength; i++) {
        float white = random(-128, 127);
        b0 = 0.99765 * b0 + white * 0.0990460;
        b1 = 0.96300 * b1 + white * 0.2965164;
        b2 = 0.57000 * b2 + white * 1.0526913;
        float pink = (b0 + b1 + b2 + white * 0.1848) * 2.0;
        pattern[i] = constrain(int(pink + 128), 0, 255);
    }
}

```

Білий шум формується як псевдовипадкова послідовність з модульованою амплітудою, а рожевий – з використанням фільтрації для досягнення спектра з переважанням нижніх частот.

Обробка команд Telegram-бота.

Користувач може взаємодіяти з пристроєм через Telegram-інтерфейс. Бот приймає наступні команди: /turnOn, /turnOff, /startWhite, /startPink.

```
void handleNewMessages(int numNewMessages) {
    for (int i = 0; i < numNewMessages; i++) {
        String text = bot.messages[i].text;
        if (text == "turnOn") noiseEnabled = true;
        if (text == "turnOff") noiseEnabled = false;
        if (text == "startWhite") useWhiteNoise = true;
        if (text == "startPink") useWhiteNoise = false;
    }
}
```

Функція перевіряє вхідні повідомлення та відповідно змінює стан системи: вмикає або вимикає шум, а також перемикає тип шуму.

Основний цикл роботи пристрою.

У головному циклі loop() здійснюється періодична перевірка Telegram-повідомлень та передавання значень шуму на DAC-виходи мікроконтролера.

```
void loop() {
    if (millis() - lastUpdate > 2000) {
        int numMessages = bot.getUpdates(bot.last_message_received + 1);
        if (numMessages) handleNewMessages(numMessages);
        lastUpdate = millis();
    }

    if (noiseEnabled) {
        uint8_t value = useWhiteNoise ? whiteNoise[noiseIndex] : pinkNoise[noiseIndex];
        dacWrite(dacPin1, value);
        dacWrite(dacPin2, value);
        noiseIndex = (noiseIndex + 1) % noiseLength;
        delayMicroseconds(random(30, 90));
    }
}
```

Завдяки інтеграції з Telegram інтерфейсом, реалізована система забезпечує дистанційне керування типом шуму, його активацією/деактивацією, а також працює в реальному часі без затримок. Telegram-керування дозволяє запускати пристрій у прихованому режимі, без необхідності фізичної взаємодії, що є критично важливим для практичного використання у режимах безперервного конфіденційного захисту.

Загалом, запрограмований код демонструє ефективну реалізацію функціональності пристрою захисту мовної інформації, заснованого на псевдовипадковому шумовому маскуванні з гнучким віддаленим керуванням.

3.2 Реалізація апаратної частини пристрою

Розробка апаратної частини пристрою захисту мовної інформації від акустичного зйому включала вибір, монтаж і тестування апаратних компонентів, необхідних для генерації акустичних завад у мовному діапазоні. Основною метою реалізації було створення компактного, енергоефективного та функціонального пристрою, здатного автономно працювати в умовах офісних або спеціалізованих приміщень.

Центральним керуючим елементом системи виступає мікроконтролер ESP32 DevKit V1, який забезпечує генерацію шуму, обробку команд користувача та передачу сигналів до підсилювального модуля. ESP32 було обрано з огляду на його високу продуктивність, наявність вбудованих DAC-портів (цифро-аналогових перетворювачів), підтримку бездротових інтерфейсів (Wi-Fi, Bluetooth), сумісність із середовищем розробки Arduino IDE, а також можливість інтеграції Telegram-бота для дистанційного керування.

Загальна електрична схема з'єднання основних компонентів пристрою представлена на рисунку 3.1. Вона демонструє принципове підключення ESP32 до підсилювача PAM8403, двох динаміків та джерела живлення, включаючи елемент ручного вмикання.

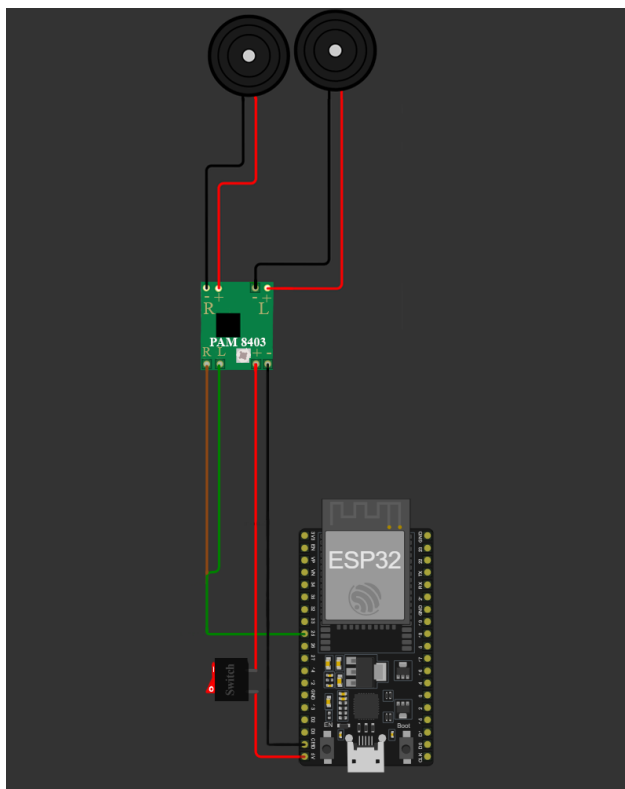


Рисунок 3.1 – Підключення ESP32

На рисунку 3.2 зображено з'єднання ESP32 із живленням та підсилювачем. Пін DAC1 (GPIO25) використовується для виведення аналогового сигналу, сформованого алгоритмом генерації шуму (білий або рожевий).

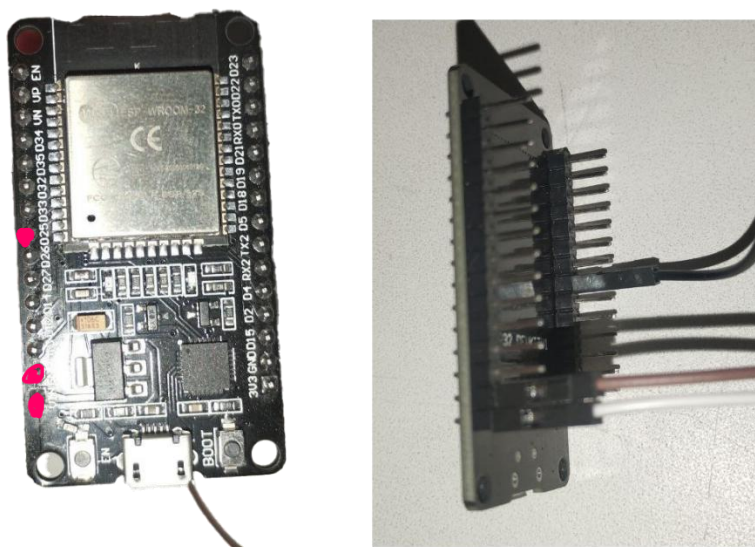


Рисунок 3.2 – Підключення ESP32

Сигнал передається на аудіопідсилювач PAM8403 (рис. 3.3), який забезпечує достатню амплітуду звукових коливань для динаміків.

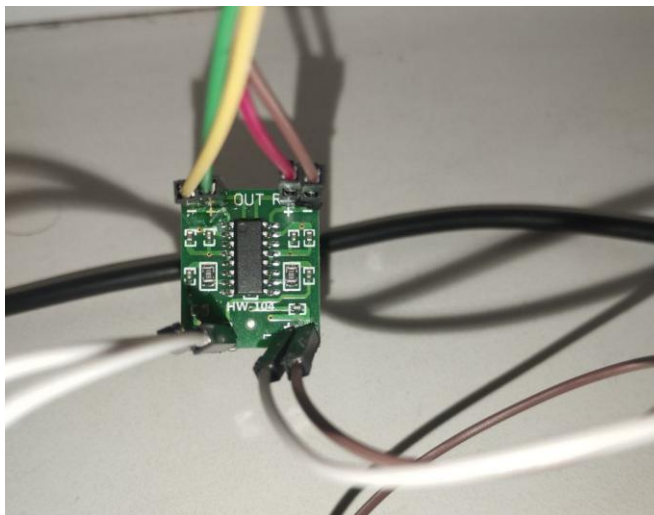


Рисунок 3.3 – З'єднання DAC з PAM8403

Модуль PAM8403 є двоканальним підсилювачем класу D, що характеризується низьким енергоспоживанням (до 3 Вт), високим ККД та компактними розмірами. Його входні лінії підключено безпосередньо до DAC ESP32, а виходи – до двох динаміків з номінальним опором 8 Ом і потужністю 2 Вт кожен (рис. 3.4). Акустичні випромінювачі забезпечують формування локального шумового поля в межах 2–3 метрів, достатнього для ефективного маскування мовлення.



Рисунок 3.4 – З'єднання DAC з PAM8403

Для автономності в конструкцію інтегровано систему живлення на 5 В, що може бути реалізована через power bank або літєвий акумулятор. Перемикач (рис.

3.5), розміщений на лінії подачі живлення до ESP32, дозволяє фізично вимикати пристрій без роз'єднання дротів.



Рисунок 3.5 – Елемент ручного вмикання пристрою

Усі з'єднання реалізовано через гнучкі Dupont-проводи, що дозволяє легко перепаявати або модифікувати пристрій. Проведено перевірку відповідності рівнів живлення, уникаючи перевищення напруги на входах ESP32 і PAM8403. Загальна схема з'єднань передбачає об'єднання ліній «землі» (GND) усіх компонентів та паралельну подачу напруги живлення до ESP32 і підсилювача.

Розпіновка основних компонентів пристрою реалізована наступним чином:

ESP32:

GPIO25 (DAC1) → IN+ підсилювача PAM8403 R+L канали
GND → загальна "земля" всіх компонентів
VCC → Switch On/Off (від esp32 до PAM8403 +)

PAM8403:

VCC → +5V (від esp32)
GND → GND esp32
IN+ → DAC1 ESP32
IN- → GND
L OUT / R OUT → "+" динаміків

Динаміки ($2 \times 8 \text{ Ом}$):

"+" → L OUT / R OUT з PAM8403
"-" → GND від PAM 8403

Після завершення монтажу та перевірки підключення всіх елементів було проведено тестування працездатності пристрою в умовах, наближених до експлуатаційних. У результаті підтверджено стабільну генерацію білого та

рожевого шуму, коректну роботу Telegram-інтерфейсу керування, а також ефективно акустичне відтворення сигналу в межах робочої зони.

Конструктивна простота (рис. 3.6), універсальність живлення та мінімальні габарити дозволяють інтегрувати пристрій у різні типи приміщень – від переговорних кімнат до польових мобільних засобів захисту. Завдяки використанню наявних бюджетних компонентів та відкритого програмного середовища Arduino, пристрій є доступним для повторення, адаптації й масштабування.



Рисунок 3.6 – Кінцевий вигляд пристрою

Таким чином, реалізована апаратна частина повністю відповідає вимогам до системи активного акустичного маскуванню та забезпечує технічну базу для подальшої інтеграції, вдосконалення та розгортання в межах комплексного захисту інформації.

3.3 Тестування ефективності пристрою

Тестування є дуже важливим етап розробки будь-якого електронного пристрою, особливо у випадках, коли йдеться про захист інформації. Метою цього етапу було підтвердження працездатності генератора шуму, перевірка

характеристик сигналу в часовій і частотній областях, оцінка рівня акустичного випромінювання, а також перевірка ефективності перекриття мовного діапазону.

Тестування проводилося за кількома напрямками:

- робота телеграм бота;
- спектральний аналіз згенерованого шуму;
- аналіз сигналів у часовій області;
- вимірювання рівня звукового тиску (гучності);
- тестування перекриття мовного сигналу;
- оцінка стабільності пристрою в часі та різних умовах живлення.

Робота телеграм бота.

Після підключення до мережі Wi-Fi пристрій автоматично ініціалізує підключення до Telegram API та надсилає повідомлення « ESP32 запущено. Надішліть /start для керування.» про готовність до роботи (рис. 3.7).

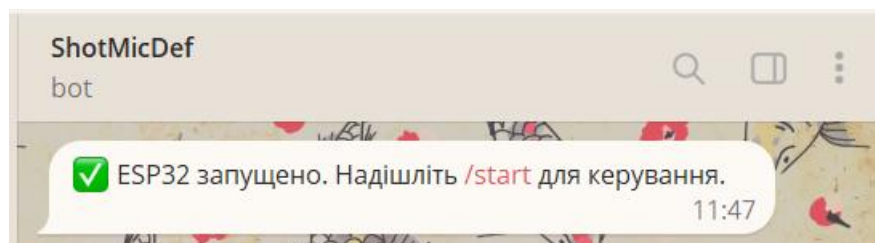


Рисунок 3.7 – Повідомлення про запуск ESP32 у Telegram

Після надсилання команди /start користувачеві відкривається інлайн-меню з чотирма варіантами для вибору режиму роботи пристрою (рис. 3.8):

- 1) « Ввімкнути»;
- 2) « Вимкнути»;
- 3) « Білий шум»;
- 4) « Рожевий шум».

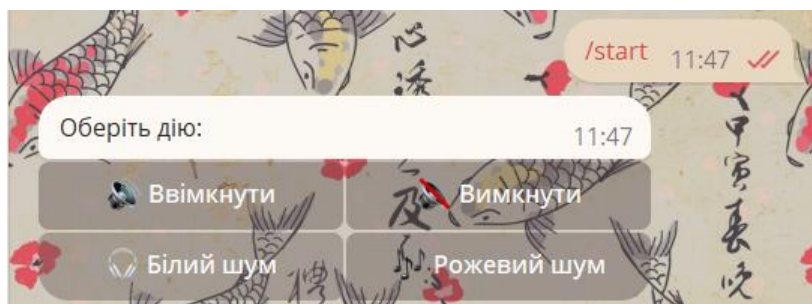


Рисунок 3.8 – Меню вибору режиму роботи через Telegram-бота

Функціональність кожної з кнопок протестовано:

«  Ввімкнути» – активує генерацію обраного шуму на обох каналах (DAC1 і DAC2). Після натискання виводиться повідомлення «Шум увімкнено.» (рис. 3.9).

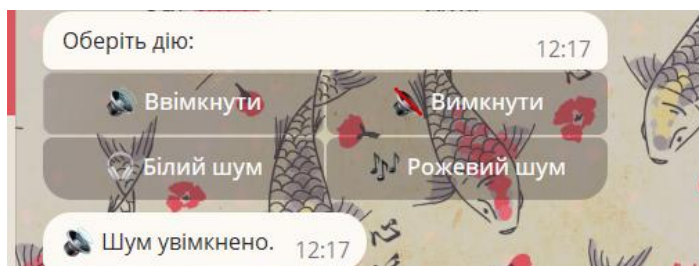


Рисунок 3.9 – Відповідь бота на команду «  Ввімкнути»

«  Вимкнути» – зупиняє генерацію шуму. Після натискання з'являється повідомлення «Шум вимкнено.» (рис. 3.11).

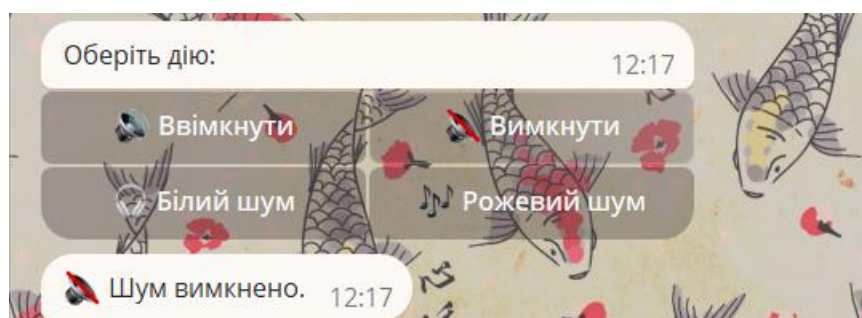


Рисунок 3.11 – Відповідь бота на команду «  Вимкнути»

«  Білий шум» – встановлює тип шуму як білий. Підтверджується повідомленням «Білий шум активовано.» (рис. 3.12).

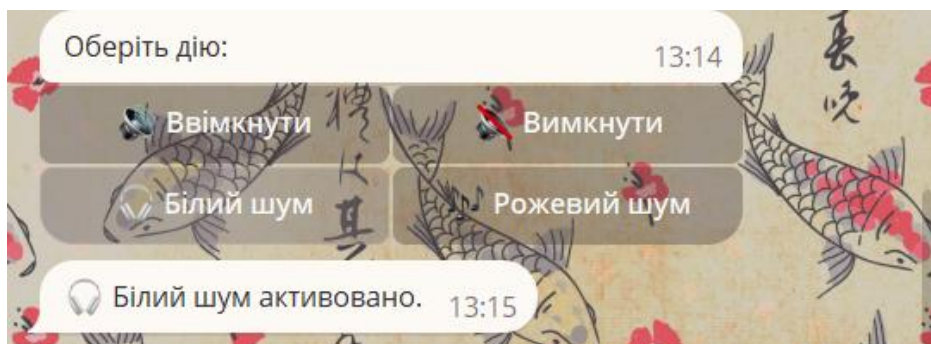


Рисунок 3.12 – Відповідь бота на команду «🔊 Білий шум»

«🎵 Рожевий шум» – перемикає генерацію на рожевий шум. Бот надсилає відповідь «Рожевий шум активовано.» (рис. 3.13).

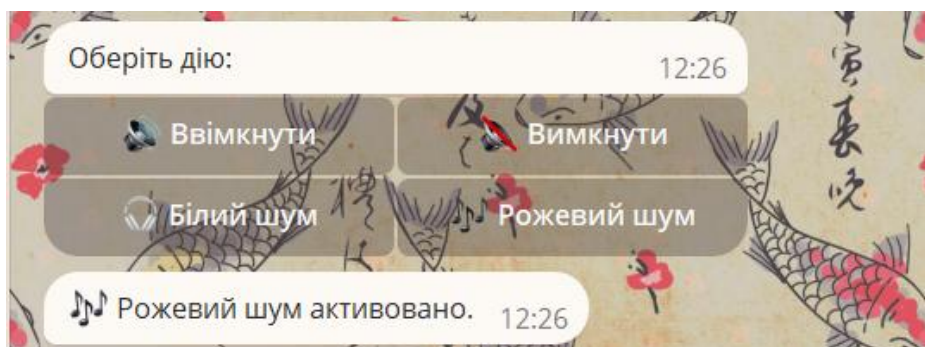


Рисунок 3.13 – Відповідь бота на команду “🎵 Рожевий шум”

Завдяки чіткому відображенню кожної дії в Telegram-боті та можливості миттєвого перемикавання режимів, користувач отримує ефективний і зручний інтерфейс контролю, що особливо важливо в умовах обмеженого фізичного доступу до пристрою або при встановленні в прихованих точках.

Тестування згенерованих шумів.

Було здійснено генерацію білого та рожевого шуму, результати якої подано у вигляді графіків сигналу у часовій області (рис. 3.14-3.15) та спектральної щільності потужності (PSD) (рис. 3.16-3.17).

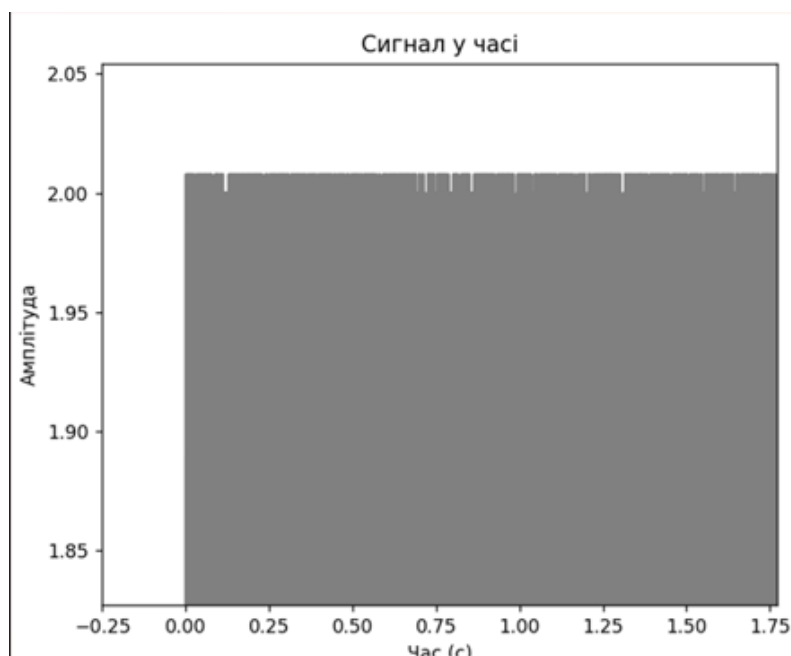


Рисунок 3.14 – Білий шум: сигнал у часовій області

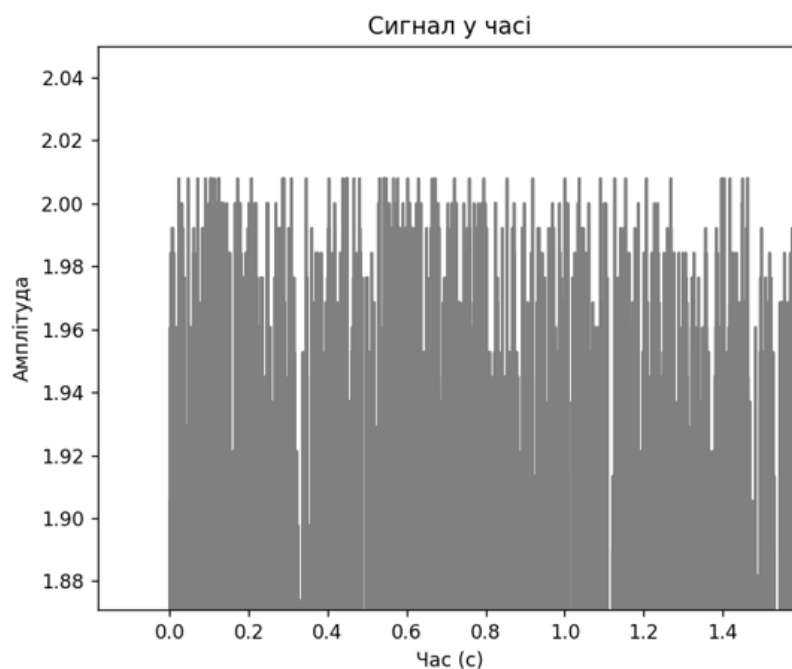


Рисунок 3.15 – Рожевий шум: сигнал у часовій області

На рисунку 3.14 представлено сигнал білого шуму у часовій області, а на рисунку 3.15 – сигнал рожевого шуму. Як видно, білий шум характеризується хаотичним, псевдовипадковим розподілом амплітуд без помітної регулярності. Сигнал має практично рівномірну насиченість, що підтверджує його здатність до перекриття мовних коливань. Натомість рожевий шум демонструє м'якші коливання з візуально більш вираженими низькочастотними компонентами, які є

типovими для $1/f$ шуму. Такий сигнал краще сприймається людським вухом і створює менш нав'язливе акустичне тло.

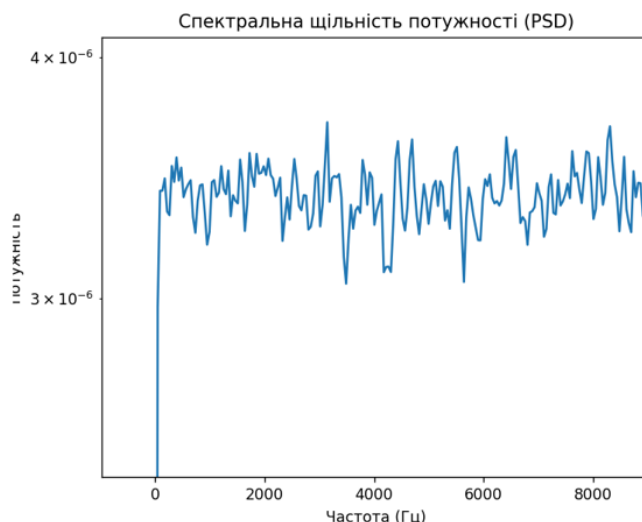


Рисунок 3.16 – PSD білого шуму

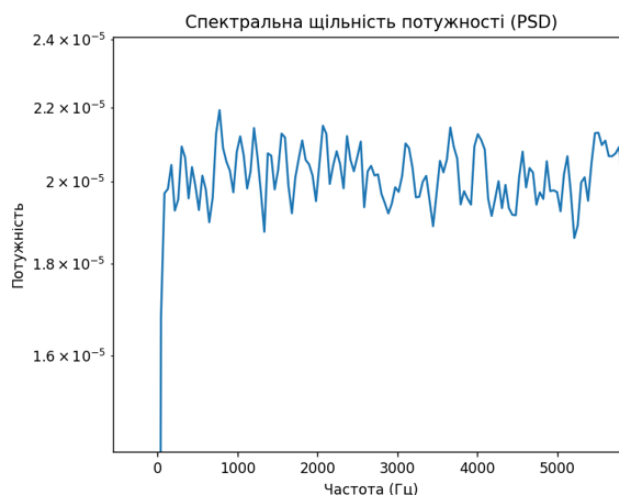


Рисунок 3.17 – PSD рожевого шуму

На рисунку 3.16 зображено графік спектральної щільності потужності (PSD) білого шуму. PSD білого шуму демонструє рівномірний розподіл енергії у всьому частотному діапазоні, без виражених піків. Це підтверджує теоретичне визначення білого шуму, як сигналу з постійною спектральною щільністю, що забезпечує ефективне маскування мовлення у всьому діапазоні частот.

На рисунку 3.17 подано PSD рожевого шуму. На відміну від білого, рожевий шум має спад потужності зі зростанням частоти, що є типовим для сигналів з інверсною спектральною щільністю ($1/f$). Це підтверджує достовірність реалізації

рожевого шуму як більш природного виду завади, який знижує навантаження на слуховий апарат людини, зберігаючи при цьому достатню ефективність маскування в діапазоні мовлення.

Вимірювання гучності.

Окрім спектрального аналізу, було проведено практичне вимірювання гучності створених шумових сигналів за допомогою цифрового шумоміра у вигляді мобільного додатку «Sound Meter» [21], встановленого на смартфон із вбудованим мікрофоном. Вимірювання виконувалося в умовах закритого приміщення площею 12 м², на відстані 1 метра від динаміків, що працювали в номінальному режимі.

Результати вимірювання:

- білий шум: середній рівень – 72 дБ, піковий – 74 дБ (рис. 3.18);
- рожевий шум: середній рівень – 70 дБ, піковий – 72 дБ (рис. 3.19).

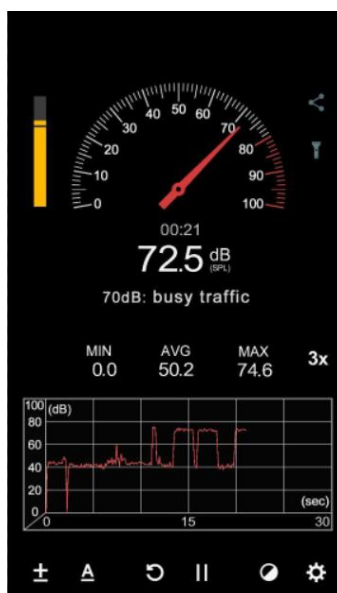


Рисунок 3.18 – Вимірювання гучності білого шуму

Зафіксоване значення гучності білого шуму склало максимум 74.6 дБ, при середньому значенні в 72 дБ. Основне значення гучності утримувалося у межах 70 – 73 дБ, що свідчить про стабільне відтворення шумового сигналу достатньої інтенсивності для ефективного захисту інформації від зйому мікрофоном направленої дії акустичним каналом. Спостерігається характерний рівномірний розподіл енергії в частотному спектрі, без різких стрибків, що відповідає властивостям білого шуму.

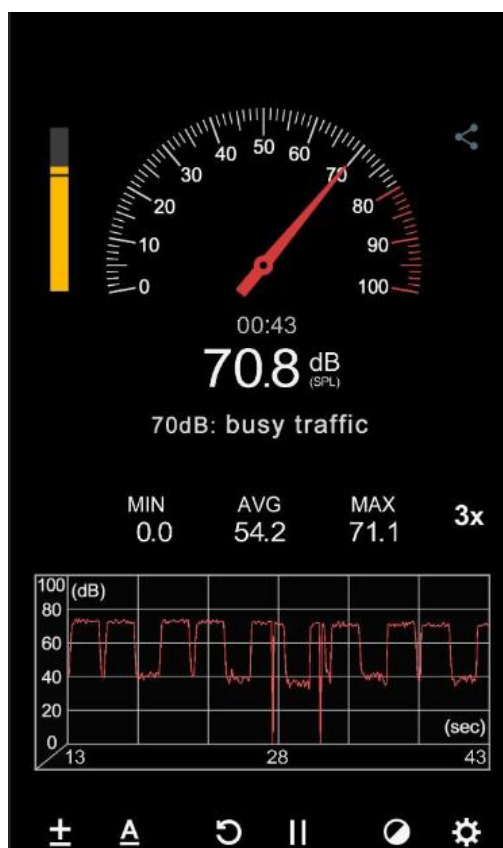


Рисунок 3.19 – Вимірювання гучності рожевого шуму

На рисунку 3.19 зафіксовано максимальну гучність 71.1 дБ при середньому рівні 70.2 дБ. Загальний характер графіку демонструє більш плавні коливання, ніж у білому шумі, що відповідає його природній акустичній структурі зі зменшенням потужності на вищих частотах. Такий шум краще сприймається людським вухом і викликає менше акустичне навантаження при тривалому впливі, водночас зберігаючи захисну ефективність.

Ці показники свідчать про безпечний рівень шуму, який не перевищує допустимих санітарних норм для тривалого перебування людини, водночас забезпечуючи ефективне екранування мовлення на рівні звичайної розмови (55–60 дБ).

Візуальне приглушення мовлення під впливом шуму.

Для додаткової перевірки ефективності пристрою було здійснено експеримент з візуалізацією звукової амплітуди мовлення при відсутності (рис. 3.20) та присутності шуму (рис. 3.21). Запис проводився за допомогою мікрофона,

підключеного до ноутбука, із наступним відображенням амплітудного сигналу в аудіо редакторі.



Рисунок 3.20 – Амплітуда голосового сигналу без шуму

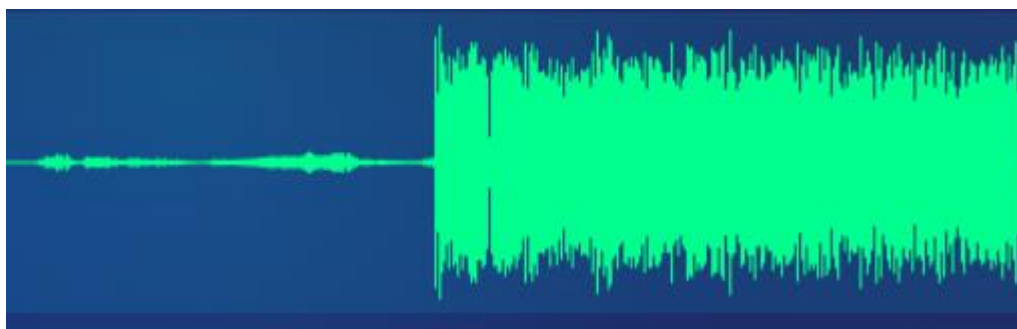


Рисунок 3.21 – Амплітуда того ж сигналу з накладеним білим шумом

Такий підхід демонструє реальне зниження розбірливості мовного сигналу при записі навіть поблизу джерела звуку. Це є ключовим показником ефективності пристрою захисту від акустичного зйому мовної інформації.

Оцінка стабільності роботи.

На основі технічних характеристик мікроконтролера ESP32 DevKit V1, підсилювача РАМ8403 та підключених динаміків було здійснено теоретичний розрахунок потужності, споживаної пристроєм у активному режимі.

Загальне енергоспоживання розраховувалося за формулою:

$$P = U \times I$$

де:

P – потужність, що споживається (Вт),

$U=5$ В – напруга живлення,

$I=0.42$ А – орієнтовна сила струму споживання (взята з типових даних ESP32 і РАМ8403 при навантаженні).

Отже:

$$P = 5 \times 0.42 = 2.1 \text{ Вт}$$

Для розрахунку тривалості автономної роботи від power bank ємністю 5000 мА·год при напрузі 5 В використовується співвідношення:

$$t = \frac{C}{I}$$

де:

t – орієнтовний час роботи (год),

$C=5000$ мА·год – ємність акумулятора,

$I=420$ мА – середня сила струму споживання.

$$t = \frac{5000}{420} = 11.9 \text{ годин}$$

Таким чином, теоретично пристрій може працювати понад 11 годин від одного заряду стандартного зовнішнього акумулятора.

Під час практичного тестування пристрій демонстрував стабільну роботу протягом понад 4 годин без перегріву, збоїв або зниження ефективності. Перемикання між режимами шуму через Telegram-бот виконувалося без затримок, що свідчить про надійність реалізованого алгоритму.

Загальні висновки за результатами тестування

Реалізований пристрій успішно генерує два типи шуму – білий та рожевий – з параметрами, що відповідають теоретичним характеристикам відповідних моделей. Це підтверджено як в часовій області, так і на основі спектрального аналізу (PSD).

Акустичний сигнал, створений пристроєм, ефективно перекриває мовний діапазон частот (300–3400 Гц). Заміряні рівні гучності (до 74 дБ) свідчать про достатню інтенсивність для маскування живої мови в реальних умовах.

Електронна схема, побудована на базі ESP32 DevKit V1, підсилювача PAM8403 та двох динаміків, демонструє стабільну роботу як при живленні від USB-адаптера, так і від портативного акумулятора ємністю 5000 мА·год. Теоретичний розрахунок показує автономність роботи понад 11 годин.

Telegram-бот, розгорнутий на платформі ESP32, забезпечує зручне дистанційне керування пристроєм у реальному часі, включаючи вибір типу шуму, активацію чи деактивацію генерації. Інтерфейс протестовано на практиці – усі команди виконуються без затримок.

Експеримент з візуальним маскуванням мовлення продемонстрував повне приглушення голосового сигналу після активації білого шуму, що підтверджує ефективність пристрою для протидії спрямованому акустичному зйому.

На основі проведеного тестування та аналізу роботи пристрою можна виокремити наступні переваги та недоліки.

Основні переваги:

- висока ефективність маскування мовлення у діапазоні частот 300–3400 Гц;
- можливість генерації двох типів шуму (білий і рожевий);
- дистанційне керування через Telegram-бот, що спрощує використання в прихованих або важкодоступних місцях;
- автономність роботи понад 11 годин при живленні від звичайного павер банка;
- стабільна робота мікроконтролера та підсилювача без перегріву чи збоїв при тривалому використанні;
- низька вартість компонентів і простота повторення конструкції.

До недоліків конструкції на поточному етапі можна віднести:

- відсутність вбудованого екрана або індикації стану, що ускладнює діагностику без доступу до Telegram;
- неможливість зберігати налаштування після втрати живлення (тип шуму завжди скидається до білого після перезапуску);
- обмежена гучність через використання 2-ватних динаміків – у великих приміщеннях ефективність маскування може зменшуватись;
- можливий дискомфорт для користувачів, що перебувають тривалий час у зоні дії пристрою.

3.4 Висновок до розділу 3

У цьому розділі було реалізовано повний цикл створення та перевірки пристрою захисту мовної інформації від зйому мікрофоном направленої дії. Розроблено та зібрано електронну схему на основі плати ESP32 DevKit V1, підсилювача РМ8403 та двох динаміків, а також впроваджено функціонал генерації білого та рожевого шуму з виводом на обидва аналогові канали DAC. Для зручності керування пристроєм реалізовано Telegram-інтерфейс з можливістю дистанційного перемикавання режимів роботи.

У процесі тестування підтверджено відповідність згенерованих шумів теоретичним характеристикам – як у часовій, так і частотній області. Білий шум демонструє рівномірну спектральну щільність, а рожевий – спад згідно з моделлю $1/f$. Вимірювання гучності засвідчили, що рівень звукового тиску перевищує середній рівень людського мовлення, забезпечуючи ефективне маскування. Експерименти з візуалізацією мовлення довели зниження розбірливості голосу під час роботи пристрою.

Розроблений програмно-апаратний комплекс продемонстрував стабільну роботу, енергоефективність та практичну придатність до використання у реальних умовах для забезпечення акустичного захисту мовної інформації.

ВИСНОВКИ

У результаті виконання даної бакалаврської кваліфікаційної роботи на тему «Розробка пристрою захисту інформації від зйому мікрофоном направленої дії акустичним каналом» було створено працюючий прототип активного засобу акустичного маскування, здатного ефективно протидіяти витoku мовної інформації.

У ході дослідження було вивчено природу витoku мовної інформації через спрямовані мікрофони, проаналізовано сучасні методи протидії таким загрозам, із-поміж яких обґрунтовано вибір активного захисту шляхом генерації шуму.

Розроблений пристрій побудований на базі мікроконтролера ESP32 DevKit V1 та підсилювача PAM8403 з двома широкосмуговими динаміками. У пристрої реалізовано генерацію білого та рожевого шуму через DAC-виходи мікроконтролера, що дозволяє створювати акустичне маскування мовного діапазону частот. Окремо розроблено Telegram-бота, який забезпечує зручне дистанційне керування пристроєм у реальному часі, включаючи можливість вибору типу шуму, його активації або вимкнення.

Під час тестування було підтверджено, що пристрій формує шумові сигнали з характеристиками, наближеними до теоретичних моделей білого та рожевого шуму. Спектральний аналіз (PSD) засвідчив рівномірний розподіл потужності для білого шуму та спад згідно з законом $1/f$ для рожевого шуму. Проведені вимірювання за допомогою цифрового шумоміра вказали на рівень гучності що є достатнім для перекриття мовлення у типовому офісному або домашньому середовищі.

Таким чином, результати тестування повністю підтвердили працездатність і ефективність розробленого пристрою як засобу активного акустичного маскування в умовах, наближених до реального використання. Отримані результати свідчать про можливість практичного застосування пристрою для захисту мовної інформації від несанкціонованого зйому спрямованими мікрофонами через акустичний канал.

ПЕРЕЛІК ПОСИЛАНЬ

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. 2016. 104 с. --К.: ІСЗІ НТУУ «КПІ», (дата звернення: 05.05.2025).
2. Методика оптимізації кількості засобів блокування каналів витоку акустичної інформації на об'єкті інформаційної діяльності. Гуменюк І., Костерев Д., Шейгас В. Ukrainian Scientific Journal of Information Security, 2025, 30(2):289-296.
3. Sennheiser MKE 600 – спрямований мікрофон [Електронний ресурс]. – Режим доступу: <https://www.sennheiser.com/en-us/catalog/products/microphones/mke-600/mke-600-505453> (дата звернення: 06.05.2025).
4. Sun-Mechatronics MW-25 – Directional Microphone [Електронний ресурс]. – Режим доступу: <https://sun-mechatronics.co.jp/EN/products/mic/mw-25.html> (дата звернення: 06.05.2025).
5. SpyFiles SPEI RMK-129 – прослуховуючий пристрій [Електронний ресурс]. – Режим доступу: https://wikileaks.org/spyfiles/files/0/164_SPEI-RMK-129.pdf (дата звернення: 08.05.2025).
6. MemoQ MQ-78 – диктофон-ручка [Електронний ресурс]. – Режим доступу: https://www.spyproworld.com/thinnest-pen-with-dictaphone-memoq-mq-78-with-1gb-memory/?utm_source=chatgpt.com (дата звернення: 09.05.2025).
7. GMD2200NEO – лазерний мікрофон [Електронний ресурс]. – Режим доступу: <https://www.detective-store.com/laser-microphone-gmd2200neo-range-up-to-300-m-picks-up-the-sound-from-any-type-of-surface-2717.html/10242> (дата звернення: 09.05.2025).
8. Tongtong Yuan, Weihong Deng, Jian Tang, Yinan Tang, Binghui Chen; Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019, pp. 4815-4824 (дата звернення: 09.05.2025).

9. Загальний огляд систем віброакустичного зашумлення [Електронний ресурс]. – Режим доступу: <https://tzi.com.ua/zagalnij-oglyad-sistem-vbroakustichnogo-zashumlennya.html> (дата звернення: 09.05.2025).

10. Acoustic modeling of shotgun microphones [Електронний ресурс]. – Режим доступу: <https://pubs.aip.org/asa/jasa/article-abstract/133/4/2036/916116/Refined-acoustic-modeling-and-analysis-of-shotgun?redirectedFrom=fulltext> (дата звернення: 12.05.2025).

11. НД ТЗІ Р 001–2000. Захист інформації [Електронний ресурс]. – Режим доступу: <https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-r-001-2000.pdf> (дата звернення: 13.05.2025).

12. Типи шуму в цифровому звуці [Електронний ресурс]. – Режим доступу: <https://emastered.com/uk/blog/different-types-of-noise> (дата звернення: 14.05.2025).

13. ESP32 Datasheet [Електронний ресурс]. – Режим доступу: <https://www.alldatasheet.com/view.jsp?Searchword=Esp32> (дата звернення: 14.05.2025).

14. PAM8403 Datasheet [Електронний ресурс]. – Режим доступу: <https://www.alldatasheet.com/datasheet-pdf/pdf/1148084/ARTSCHIP/PAM8403.html> (дата звернення: 14.05.2025).

15. Arduino IDE Software [Електронний ресурс]. – Режим доступу: <https://www.arduino.cc/en/software/> (дата звернення: 14.05.2025).

16. Arduino-ESP32 документація [Електронний ресурс]. – Режим доступу: <https://docs.espressif.com/projects/arduino-esp32/en/latest/installing.html> (дата звернення: 14.05.2025).

17. ESP32 espressif [Електронний ресурс]. – <https://docs.espressif.com/projects-arduino-esp32/en/latest/installing.html> 14.05.2025).

18. Universal Telegram Bot Library [Електронний ресурс]. – Режим доступу: <https://www.arduino-libraries.info/libraries/universal-telegram-bot> (дата звернення: 16.05.2025).

19. Arduino ESP32 Documentation [Электронный ресурс]. – Режим доступа: <https://docs.espressif.com/projects/arduino-esp32/en/latest/installing.html> (дата звернения: 16.05.2025).

20. Arduino Cloud for ESP32 [Электронный ресурс]. – Режим доступа: <https://docs.arduino.cc/arduino-cloud/guides/arduino-c/> (дата звернения: 16.05.2025).

21. Sound Meter [Электронный ресурс]. – Режим доступа: <https://play.google.com/store/apps/details?id=com.gamebasic.decibel> (дата звернения: 18.05.2025).

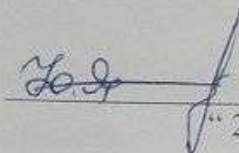
ДОДАТКИ

Додаток А. Технічне завдання

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

ЗАТВЕРДЖУЮ

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

 Юрій ЯРЕМЧУК
“ 20 ” березня 2025 р.

ТЕХНІЧНЕ ЗАВДАННЯ

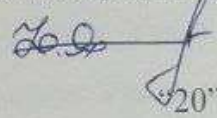
до бакалаврської кваліфікаційної роботи на тему:

Розробка пристрою захисту інформації від зйому мікрофоном направленої дії
акустичним каналом

08-72.БДР.017.00.058 ТЗ

Керівник бакалаврської кваліфікаційної роботи

д.т.н., професор кафедри МБІС

 Яремчук Ю.Є.
“ 20 ” березня 2025 р.

Вінниця – 2025 р.

1. Найменування та область застосування

Програмний засіб методу захисту від атаки типу прослуховування. Область застосування: захист акустичної інформації від несанкціонованого доступу шляхом використання мікрофонів направленої дії.

2. Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ № 97 від 20.03.2025 р.

3. Мета та призначення розробки

3.1 Мета розробки: розробка та виготовлення пристрою для захисту інформації від зйому мікрофоном направленої дії шляхом створення спрямованої шумової завади.

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

4. Джерела розробки

4.1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. 2016. 104 с. --К.: ІСЗЗІ НТУУ «КПІ», (дата звернення: 05.05.2025).

4.2. Методика оптимізації кількості засобів блокування каналів витоку акустичної інформації на об'єкті інформаційної діяльності. Гуменюк І., Костерев Д., Шейгас В. Ukrainian Scientific Journal of Information Security, 2025, 30(2):289-296.

4.3. Tongtong Yuan, Weihong Deng, Jian Tang, Yinan Tang, Binghui Chen; Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019, pp. 4815–4824 (дата звернення: 09.05.2025).

4.4. Загальний огляд систем віброакустичного зашумлення [Електронний ресурс]. – Режим доступу: <https://tzi.com.ua/zagalnij-oglyad-sistem-vbroakustichnogo-zashumlennya.html> (дата звернення: 09.05.2025).

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

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

5.1.2 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків;

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.2 Програмний засіб повинен виконувати свої функції.

6. Вимоги до програмної документації

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

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист розроблюваного програмного засобу від несанкціонованого використання.

7.2 Неможливість користування інтерфейсом після його блокування програмним модулем захисту.

8. Техніко– економічні показники

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

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

9. Стадії та етапи розробки

№ з/п	Назва етапів бакалаврської кваліфікаційної роботи	Початок	Закінчення
1.	Визначення напрямку бакалаврської роботи, формулювання теми	10.03.2025	15.03.2025
2.	Аналіз предметної області обраної теми	20.03.2025	19.04.2025
3.	Розробка алгоритму роботи	11.05.2025	20.05.2025
4.	Написання бакалаврської роботи на основі розробленої теми	21.05.2025	25.05.2025

5.	Передзахист бакалаврської кваліфікаційної роботи	27.05.2025	28.05.2025
6.	Виправлення, уточнення, корегування бакалаврської кваліфікаційної роботи	29.05.2025	29.05.2025
7.	Захист бакалаврської кваліфікаційної роботи	10.06.2025	11.06.2025

10. Порядок контролю та прийому

10.1 До приймання бакалаврської кваліфікаційної роботи надається:

- ПЗ до бакалаврської кваліфікаційної роботи;
- демонстрація результату бакалаврської кваліфікаційної роботи;
- презентація;
- відзив керівника роботи;
- відзив рецензента

Технічне завдання до виконання прийняв Р.С. Соколовський Д.С.

Додаток Б. Лістинг програмного коду

```

#include <WiFi.h>
#include <WiFiClientSecure.h>
#include <UniversalTelegramBot.h>
#include <ArduinoJson.h>

// --- Налаштування Wi-Fi ---
const char* ssid = "a0811 2.0";
const char* password = "+380673386714";

// --- Telegram Bot ---
#define BOT_TOKEN "7416292004:AAFQNu6bxxElzBRzsdvclsVKO7fmO47qZkY"
#define CHAT_ID "706406607"

WiFiClientSecure client;
UniversalTelegramBot bot(BOT_TOKEN, client);

// --- Виводи DAC ---
const int dacPin1 = 25;
const int dacPin2 = 26;

const int noiseLength = 512;
uint8_t whiteNoise[noiseLength];
uint8_t pinkNoise[noiseLength];
int noiseIndex = 0;

bool noiseEnabled = false;
bool useWhiteNoise = true;

unsigned long lastUpdate = 0;

// --- Генерація білого шуму ---
void generateWhiteNoise(uint8_t* pattern) {
  for (int i = 0; i < noiseLength; i++) {
    int base = random(100, 220); // підвищена амплітуда
    int modulation = random(-30, 30);
    pattern[i] = constrain(base + modulation, 0, 255);
  }
}

// --- Генерація рожевого шуму (1/f шум) ---
void generatePinkNoise(uint8_t* pattern) {
  float b0 = 0, b1 = 0, b2 = 0;
  for (int i = 0; i < noiseLength; i++) {
    float white = random(-128, 127);
    b0 = 0.99765 * b0 + white * 0.0990460;
    b1 = 0.96300 * b1 + white * 0.2965164;
    b2 = 0.57000 * b2 + white * 1.0526913;
    float pink = (b0 + b1 + b2 + white * 0.1848) * 2.0; // підсилення
    pattern[i] = constrain(int(pink + 128), 0, 255);
  }
}

// --- Обробка Telegram-команд ---
void handleNewMessages(int numNewMessages) {
  for (int i = 0; i < numNewMessages; i++) {

```

```

String text = bot.messages[i].text;
String chat_id = bot.messages[i].chat_id;

if (text == "/start") {
    String keyboardJson = "[[{ \"text\": \"🔊 Ввімкнути\", \"callback_data\": \"turnOn\" },"
        "{ \"text\": \"🔇 Вимкнути\", \"callback_data\": \"turnOff\" }],\"
        \"[{ \"text\": \"🎧 Білий шум\", \"callback_data\": \"startWhite\" },\"
        \"{ \"text\": \"🎵 Рожевий шум\", \"callback_data\": \"startPink\" }]]\";
    bot.sendMessageWithInlineKeyboard(chat_id, "Оберіть дію:", "", keyboardJson);
}

if (text == "turnOn") {
    noiseEnabled = true;
    bot.sendMessage(chat_id, "🔊 Шум увімкнено.");
}
if (text == "turnOff") {
    noiseEnabled = false;
    bot.sendMessage(chat_id, "🔇 Шум вимкнено.");
}
if (text == "startWhite") {
    useWhiteNoise = true;
    bot.sendMessage(chat_id, "🎧 Білий шум активовано.");
}
if (text == "startPink") {
    useWhiteNoise = false;
    bot.sendMessage(chat_id, "🎵 Рожевий шум активовано.");
}
}
}

// --- Підключення Wi-Fi ---
void connectWiFi() {
    WiFi.begin(ssid, password);
    while (WiFi.status() != WL_CONNECTED) {
        delay(500);
    }
    client.setInsecure(); // без сертифікатів
}

// --- Початок роботи ---
void setup() {
    Serial.begin(115200);
    connectWiFi();

    generateWhiteNoise(whiteNoise);
    generatePinkNoise(pinkNoise);

    bot.sendMessage(CHAT_ID, "✅ ESP32 запущено. Надішліть /start для керування.");
}

// --- Основний цикл ---
void loop() {
    if (millis() - lastUpdate > 2000) {
        int numMessages = bot.getUpdates(bot.last_message_received + 1);
        if (numMessages) {
            handleNewMessages(numMessages);
        }
    }
}

```

```
    lastUpdate = millis();  
  }  
  
  if (noiseEnabled) {  
    uint8_t value = useWhiteNoise ? whiteNoise[noiseIndex] : pinkNoise[noiseIndex];  
    dacWrite(dacPin1, value);  
    dacWrite(dacPin2, value);  
    noiseIndex = (noiseIndex + 1) % noiseLength;  
  
    delayMicroseconds(random(30, 90)); // швидке оновлення для гучності  
  }  
}
```

Додаток В. Ілюстраційний матеріал

Розробка пристрою захисту інформації від зйому мікрофоном направленої дії акустичним каналом

Виконав студент групи 2КІТС-21Б Соколовський Дмитро Сергійович
Науковий керівник д.т.н., професор кафедри МБІС Яремчук Юрій Євгенович

1

АКТУАЛЬНІСТЬ ТЕМИ

У сучасних умовах акустичний зйом мовної інформації за допомогою спрямованих мікрофонів є реальною загрозою безпеці.

Існує потреба у простому, доступному та ефективному засобі активного захисту, здатному перекривати акустичний канал через генерацію шуму.

Особливої актуальності набувають пристрої, здатні працювати автономно, дистанційно керовані та адаптовані до реальних умов застосування.

2

МЕТА РОБОТИ

Метою даної роботи - є розробка пристрою для захисту інформації від зйому мікрофоном направленої дії акустичним каналом

- Дослідити сучасні технічні канали витоку акустичної інформації та методи протидії їм.
- Реалізувати прототип генератора шуму для захисту інформації від зйому мікрофоном направленої дії акустичним каналом
- Провести тестування пристрою з оцінкою ефективності маскування мовного сигналу.

ВНТУ | 2025

4

МЕТА РОБОТИ

ВНТУ | 2025

Предмет дослідження:

структура, принцип дії та функціональні можливості пристрою активного акустичного маскування, реалізованого на базі мікроконтролера ESP32.

Об'єкт дослідження:

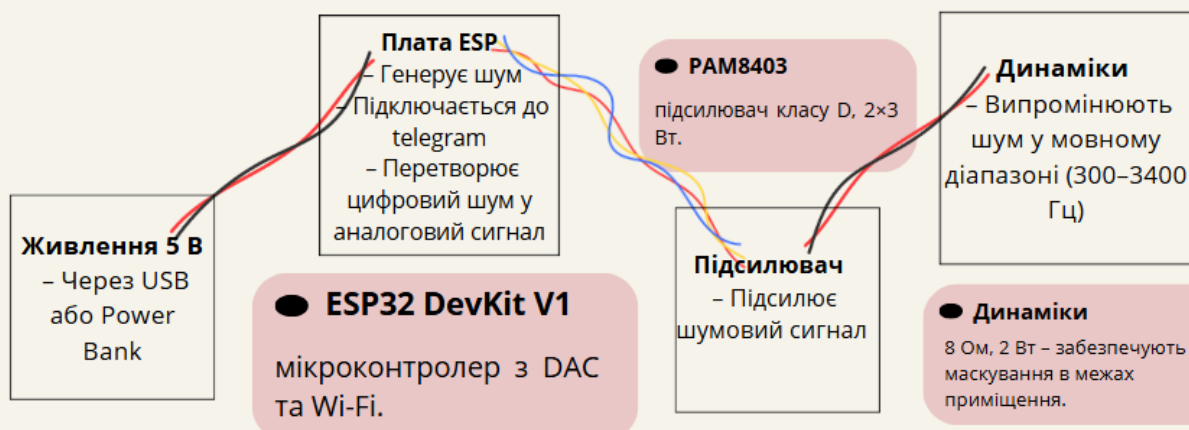
процес захисту мовної інформації від несанкціонованого перехоплення за допомогою спрямованих мікрофонів через акустичні канали.

Практична цінність

полягає у створенні пристрою для захисту мовної інформації в умовах можливого акустичного зйому.

СТРУКТУРНА СХЕМА ПРИСТРОЮ

6



ВНТУ | 2025

ПРИНЦИПИ ДІЇ ЗАХИСНИХ ПРИСТРОЇВ

5

1

Активний захист (шумове маскування)

Генерує спеціальний шум у мовному діапазоні (300–3400 Гц), що унеможливує перехоплення голосової інформації спрямованими мікрофонами.

2

Пасивний захист (екранування)

Використання матеріалів, що поглинають або відбивають звукові хвилі, обмежуючи їх поширення за межі приміщення.

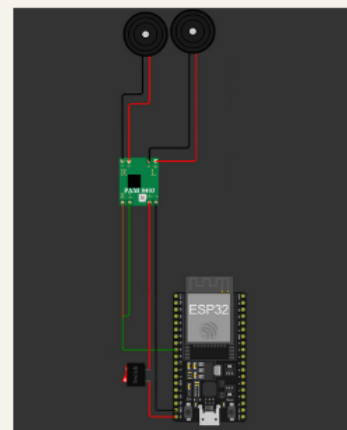
ВНТУ | 2025



7

ПРИНЦИП ДІЇ ПРИСТРОЮ

- Після запуску ESP32 підключається до Wi-Fi.
- Користувач обирає режим у Telegram (вкл/викл, білий/рожевий шум).
- На основі обраного режиму генерується псевдовипадковий шум.
- DAC ESP32 формує аналоговий сигнал, який підсилюється PAM8403.
- Акустичний сигнал маскує мовлення в реальному часі.



ВНТУ | 2025

8

РОЗРОБЛЕНИЙ ЗРАЗОК



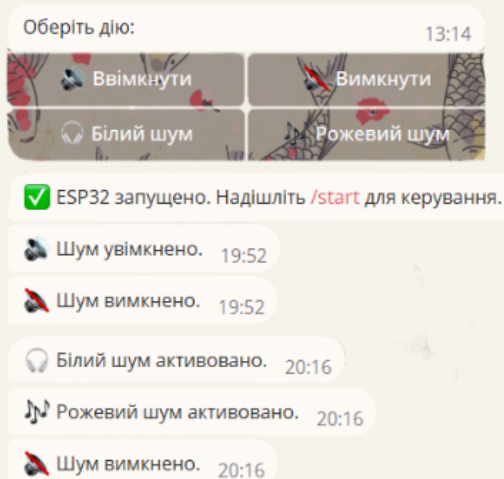
На світлинах зображений прототип пристрою готовий до використання

ВНТУ | 2025

9

ІНТЕРФЕЙС КОРИСТУВАЧА

ВНТУ | 2025



Для роботи з пристроєм був розроблений телеграм бот при підключенні до якого користувач має змогу за допомогою wi-fi вмикати вимикати пристрій та змінювати типу шуму

10

ТЕСТУВАННЯ

♦ Графіки PSD та часові діаграми

підтверджують відповідність характеристикам білого/рожевого шуму

♦ Вимірювання гучності:

- Білий шум: до 74.6 дБ
- Рожевий шум: до 71.1 дБ

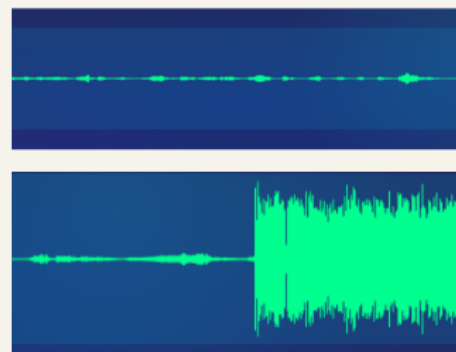
♦ Автономність:

До 11 годин роботи від павербанка (5000 мА·год)

♦ Управління:

Telegram-бот: миттєвий контроль, перемикавання шумів

♦ Приглушення мовлення:



ВНТУ | 2025

ВИСНОВКИ

У ході виконання бакалаврської роботи було проаналізовано загрози, пов'язані з витоком мовної інформації через акустичні канали, та досліджено методи її захисту.

Розроблено функціональний пристрій активного акустичного маскування на базі мікроконтролера ESP32.

Проведено тестування пристрою, яке підтвердило ефективність маскування мовлення, відповідність спектральних характеристик теоретичним моделям і стабільну роботу пристрою в автономному режимі.

Отримані результати демонструють практичну доцільність використання пристрою як доступного й ефективного засобу захисту мовної інформації від перехоплення мікрофонами направленої дії шляхом акустичного каналу.

ВНТУ | 2025

ВНТУ | 2025

**ДЯКУЮ
ЗА УВАГУ**

Соколовський Д.С.

ПРОТОКОЛ ПЕРЕВІРКИ НАВЧАЛЬНОЇ (КВАЛІФІКАЦІЙНОЇ) РОБОТИ

Назва роботи:

розробка пристрою захисту інформації від зйому мікрофоном направленої дні акустичним каналом

Тип роботи: бакалаврська кваліфікаційна робота

Підрозділ Кафедра менеджменту на безпеки інформаційних систем

Факультет менеджменту та інформаційної безпеки

Гр. 2КІТС-216

Керівник професор Яремчук Ю.Є.

Показники звіту подібності

Strike Plagiarism

Оригінальність	98,88%
Загальна схожість	1,12%

Аналіз звіту подібності (відмітити потрібне)

- ☐ Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.
- ☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її автора. Роботу направити на доопрацювання.
- ☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Заявляю, що ознайомлений (-на) з повним звітом подібності, який був згенерований Системою щодо роботи (подається)

Автор Роса
(підпис)

Соколовський Д.С.
(прізвище, ініціали)

Опис прийнятого рішення

- ☐ Допустити до захисту

Особа, відповідальна за перевірку

(підпис)

Коваль Н.П.
(прізвище, ініціали)

Експерт
(за потреби)

(підпис)

(прізвище, ініціали, посада)