МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ДЕНИСЮК ВЯЧЕСЛАВ ВОЛОДИМИРОВИЧ

Допускається до захисту:
В.о. завідувача кафедри
прикладної математики та
кібербезпеки, доктор філософії з
математики
_____Луценко А. В.
«__»_____20__ р.

МЕТОДИ ТА СПОСОБИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ МОВНОЇ ІНФОРМАЦІЇ В САЛОНІ АВТОМОБІЛЯ

Спеціальність 105 Прикладна фізика та наноматеріали

Кваліфікаційна (магістерська) робота

Науковий керівник:
Л. В. Загоруйко,
к.т.н., доцент,
доцент кафедри прикладної
математики та кібербезпеки
_____
(підпис)

Оцінка:___/___/_____
(бали за шкалою ЄКТС/за національною шкалою)
Голова ЕК:_____
(підпис)

Вінниця – 2025

АНОТАЦІЯ

Денисюк В.В. Методи та засоби захисту конфіденційної мовної інформації в салоні автомобіля. Спеціальність 105 «Прикладна фізика та наноматеріали», Освітня програма «Технології інтернету речей». Донецький національний університет імені Василя Стуса, Вінниця, 2025.

У кваліфікаційній (магістерській) роботі досліджено проблему витоку конфіденційної мовної інформації в салоні автомобіля через акустичні, віброакустичні, електронні та телематичні канали. Проаналізовано сучасні технології шумопоглинання та активного акустичного маскування, що використовуються у транспортних засобах провідних виробників (Bose, HARMAN, Continental, Panasonic, Tesla тощо). Виконано експериментальні дослідження двох систем активного захисту мовної інформації із вимірюванням словесної розбірливості в 10 контрольних точках автомобіля на трьох відстанях (10, 40, 80 см). На основі отриманих результатів розроблено гібридну систему захисту HAS-Drive, що поєднує активне віброакустичне маскування, пасивне екранування та інтелектуальне адаптивне керування шумогенерацією (VAD-аналіз, фазова корекція, адаптивний контроль потужності). Запропонована система забезпечує зниження словесної розбірливості до 15 %, що відповідає інтегральному коефіцієнту зниження 82,6 %, та перевищує ефективність існуючих рішень. Представлено математичні моделі, структурну архітектуру, енергетичний аналіз та рекомендації щодо інтеграції системи в електронну архітектуру автомобіля.

Ключові слова: мовна інформація, акустичний витік, віброакустичне маскування, активний захист, VAD, шумогенерація, автомобільна кібербезпека.

79 с., 9 табл., 10 рис., 30 джерел.

Denysiuk V. V. Methods and means of protecting confidential speech information inside a vehicle cabin. Specialty 105 “Applied Physics and Nanomaterials”, Educational program “Internet of Things Technologies”. Vasyl’ Stus

Donetsk National University, Vinnytsia, 2025.

The qualification (master's) thesis investigates the problem of confidential speech information leakage inside a vehicle cabin through acoustic, vibro-acoustic, electronic, and telematic channels. Modern technologies of noise absorption and active acoustic masking used in vehicles of leading manufacturers (Bose, HARMAN, Continental, Panasonic, Tesla, etc.) are analyzed. Experimental studies of two active speech protection systems were conducted, including measurement of speech intelligibility in 10 control points of the vehicle at three distances (10, 40, 80 cm). Based on the obtained results, a hybrid protection system HAS-Drive was developed, combining active vibro-acoustic masking, passive shielding, and intelligent adaptive noise-control algorithms (VAD processing, phase correction, adaptive power distribution). The proposed system reduces speech intelligibility to 15%, which corresponds to an 82.6% reduction coefficient, outperforming existing solutions. The thesis presents mathematical models, structural and hardware architecture, energy analysis, and recommendations for integration of the system into the vehicle's electronic architecture.

Keywords: speech information, acoustic leakage, vibro-acoustic masking, active protection, VAD, noise generation, automotive cybersecurity.

79 pp., 9 tables, 10 figures, 30 sources.

ЗМІСТ

ВСТУП 6

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА МЕТОДИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В САЛОНІ АВТОМОБІЛЯ 9

1.1 Поняття конфіденційної мовної інформації 9

1.2 Потенційні загрози для мовної інформації в салоні автомобіля 12

1.3 Основні канали витоку мовної інформації 15

1.4. Методи та способи захисту конфіденційної мовної інформації в салоні автомобіля 18

РОЗДІЛ 2. МОДЕЛЮВАННЯ ЗАГРОЗ І АНАЛІЗ ІСНУЮЧИХ СИСТЕМ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В САЛОНІ АВТОМОБІЛЯ 21

2.1 Аналіз сучасних технологій та систем у сфері захисту мовної інформації в салоні автомобіля 21

2.2 Приклади технічних засобів прослуховування (спеціальні та побутові) ... 26

2.3. Аналіз вразливостей голосових помічників та інформаційно-розважальних систем у салоні автомобіля 30

РОЗДІЛ 3. ПРАКТИЧНЕ ДОСЛІДЖЕННЯ: МОДЕЛЮВАННЯ ЗАГРОЗ І МЕТОДІВ ЗАХИСТУ 35

3.1. Вибір об’єкта дослідження та опис експериментального середовища 35

3.2 Ідентифікація та кількісна оцінка вразливих каналів витоку інформації .. 38

3.3. Результати вимірювання початкової вразливості 41

3.4. Експеримент із Системою захисту №1 43

3.5. Експеримент із Системою захисту №2 48

3.6. Порівняльний аналіз ефективності систем 54

РОЗДІЛ 4. ПРОЄКТ ГІБРИДНОЇ СИСТЕМИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В САЛОНІ АВТОМОБІЛЯ 58

4.1. Вимоги, архітектурні принципи та модель загроз 58

4.2. Структурна та апаратна архітектура системи 61

4.3. Алгоритмічне ядро системи 63

4.4. Моделювання ефективності гібридної системи 68

4.5. Інтеграція системи в архітектуру автомобіля та комерційна реалізація ... 71

ВИСНОВОК 75

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 78

ВСТУП

У сучасному світі мовна інформація є одним із ключових каналів обміну даними між людьми, що забезпечує ефективну взаємодію у діловій, технічній та особистій сферах. Проте саме її акустична природа робить мовну інформацію одним із найбільш уразливих об’єктів несанкціонованого перехоплення. У контексті розвитку мобільності та цифровізації середовищ спілкування, все частіше комунікації відбуваються поза межами захищених приміщень – зокрема, в салоні автомобіля, який дедалі частіше використовується як тимчасовий офіс або місце проведення конфіденційних переговорів [5].

Сучасний автомобіль — це складна кіберфізична система, інтегрована у глобальні телематичні мережі, що містить десятки мікрофонів, бездротових інтерфейсів (Bluetooth, Wi-Fi, LTE) та компонентів із функціями голосового управління. Такі елементи, як інформаційно-розважальні системи, голосові асистенти або телематичні модулі, потенційно можуть виступати каналами витоку конфіденційної мовної інформації (КМІ). Водночас акустичні коливання, які генеруються під час розмови, здатні поширюватися крізь скління, металеві панелі кузова чи вентиляційні системи, формуючи віброакустичні канали витоку [3].

Проблема захисту мовної інформації у салоні автомобіля має комплексний характер, оскільки поєднує фізичні, технічні, організаційні та програмні аспекти. З одного боку, розвиваються методи активного маскування, віброакустичного глушіння та цифрового шифрування мовних сигналів; з іншого — зростає інтелектуальність атак, заснованих на IoT-технологіях, дистанційному доступі та використанні машинного навчання для відновлення мовлення з побічних коливань [4].

Захист КМІ у транспортних засобах регламентується положеннями міжнародних стандартів:

- ISO/IEC 27001:2022 — Системи управління інформаційною безпекою;
- ISO 5127:2017 — Інформація та документація. Словник термінів;

- ДСТУ 3396.0–96 — Захист інформації. Основні положення;
- ДСТУ IEC TR 30164:2023 — Інтернет речей. Концепції безпеки [1-5].

Водночас чинні стандарти недостатньо враховують особливості акустичних та віброакустичних каналів у замкнутих просторах транспортних засобів, що актуалізує проведення спеціальних експериментальних досліджень [4].

Актуальність теми полягає у зростаючій потребі забезпечення конфіденційності мовних переговорів у мобільному середовищі, зокрема в автомобільному салоні, де наявність численних мікрофонів, сенсорів та каналів зв'язку створює підвищені ризики несанкціонованого доступу до інформації.

Мета дослідження — підвищення рівня захищеності конфіденційної мовної інформації в салоні автомобіля шляхом аналізу, моделювання та експериментального оцінювання ефективності сучасних методів і систем акустичного маскування [3].

Завдання дослідження:

- Проаналізувати потенційні загрози та канали витоку мовної інформації у салоні автомобіля.
- Дослідити сучасні технології активного та пасивного захисту мовних сигналів.
- Провести моделювання поширення віброакустичних сигналів у конструкції автомобіля.
- Виконати експериментальне дослідження ефективності різних систем маскування.
- Розробити пропозиції щодо створення гібридної системи захисту мовної інформації.

Об'єкт дослідження — процес передавання та поширення мовної інформації в салоні автомобіля.

Предмет дослідження — методи, способи та технічні засоби захисту конфіденційної мовної інформації від витоку через акустичні та віброакустичні канали.

Методи дослідження: теоретичний аналіз літературних джерел та стандартів, моделювання віброакустичних процесів, експериментальні вимірювання за допомогою апаратури ST031 «Піранья», статистична обробка результатів та порівняльний аналіз ефективності систем [4].

Наукова новизна роботи полягає у формуванні комплексної моделі захисту мовної інформації в салоні автомобіля з урахуванням фізичних параметрів кузова, характеристик акустичного середовища та ефективності активних систем маскування.

Практичне значення полягає у можливості використання результатів дослідження під час розробки інтегрованих систем безпеки автомобілів, а також у створенні рекомендацій для підвищення акустичної конфіденційності транспортних засобів корпоративного та спеціального призначення.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ТА МЕТОДИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В САЛОНІ АВТОМОБІЛЯ

1.1 Поняття конфіденційної мовної інформації

У сучасних системах обміну даними мовна інформація (МІ) виступає базовим засобом передачі змістовних повідомлень між людьми та технічними пристроями. Вона є різновидом акустичної інформації, що формується, передається та сприймається через коливання повітряного середовища у звуковому діапазоні частот $f = 20 \div 20000$ Гц. На відміну від текстової чи візуальної, мовна інформація має динамічну природу та високу енергетичну насиченість, що обумовлює специфіку її захисту [4].

Згідно з ДСТУ 3396.0–96 «Захист інформації. Основні положення», мовна інформація розглядається як різновид інформації, що передається акустичними сигналами у звуковому або ультразвуковому діапазоні та сприймається органами слуху людини або технічними засобами [2].

Відповідно до ISO/IEC 27001:2022, інформація вважається конфіденційною, якщо її розголошення може завдати шкоди власнику, користувачу чи третій стороні [1].

Таким чином, конфіденційна мовна інформація (КМІ) — це акустичний сигнал, що несе смислове навантаження і має обмежений доступ у зв’язку з потенційними наслідками його розголошення.

КМІ може бути класифікована за кількома критеріями:

1. За сферою використання:
    - державна — переговори, що містять інформацію з грифом “таємно” або “цілком таємно”;
    - комерційна — відомості про фінансову діяльність, контракти, стратегії компаній;

- службова — внутрішні документи, кадрові питання, управлінські рішення;
- персональна — приватні розмови, медичні або фінансові дані осіб [11].

2. За формою представлення:
   - природна мова (голос людини);
   - синтезоване мовлення (штучні голосові помічники, TTS-системи);
   - закодоване мовлення (передача голосу через цифрові канали з кодуванням або шифруванням).
3. За рівнем доступу:
   - відкритий (необмежений);
   - службовий (для обмеженого кола осіб);
   - конфіденційний;
   - секретний [1].

Для формалізації характеристик мовного сигналу розглянемо його як випадковий процес $s(t)$, що описує акустичні коливання у часі.

Енергетична потужність сигналу визначається як:

$$P_s = \frac{1}{T}\int_0^T s^2(t)dt,$$

а середньоквадратичне значення амплітуди:

$$A_{cp} = \sqrt{P_s}.$$

Інформативність мовного сигналу залежить від його ентропії, що характеризує ступінь невизначеності повідомлення:

$$H = -\sum_{i=1}^{n} p_i log_2 p_i,$$

де p_i— імовірність появи окремого елемента мовного повідомлення (фонеми, слова). Висока ентропія відповідає більш насиченому та непередбачуваному сигналу, що ускладнює його перехоплення або реконструкцію [7].

На відміну від даних у цифровому вигляді, мовна інформація має такі особливості:

- **нелокальність** — звук поширюється у середовищі без фізичних обмежень, що уможливлює його перехоплення на відстані;
- **відсутність маркерів доступу** — неможливо встановити, хто і коли "отримав" мовну інформацію;
- **відкритість каналів передачі** — акустичні та віброакустичні хвилі можуть бути зняті мікрофонами, лазерними сенсорами, структурними перетворювачами;
- **складність контролю витоку** — після проголошення повідомлення його неможливо "видалити" [8].

Для віднесення мовного сигналу до категорії конфіденційного можуть використовуватись такі критерії:

1. **Імовірність витоку**

$$P_v = f\left(A_s, D, \frac{S}{N}\right)$$

де A_s – амплітуда сигналу, D – відстань до межі салону, $\frac{S}{N}$ – відношення сигнал/шум. При $P_v > 0.5$ канал вважається небезпечним.

2. **Коефіцієнт розбірливості мовлення (Speech Intelligibility, R_s)**

$$R_s = \frac{N_{\text{пр}}}{N_{\text{заг}}} \times 100\%,$$

де $N_{\text{пр}}$ – кількість правильно розпізнаних слів, $N_{\text{заг}}$ – загальна кількість переданих слів. Якщо $R_s > 50\%$, можливе часткове відновлення змісту розмови; якщо $R_s > 70\%$ – повне.

3. **Рівень мовної захищеності ($K_з$)**

$$К_з = 1 - \frac{R_s}{100},$$

що відображає зниження доступності мовного змісту внаслідок дії системи захисту.

Мовна інформація є унікальним носієм змістових відомостей, який поєднує фізичні (акустичні) та семантичні характеристики. Її конфіденційність визначається не лише змістом повідомлення, а й умовами його передавання.

Зважаючи на зростання кількості електронних і віброакустичних каналів у салоні автомобіля, необхідність у **комплексному захисті мовної інформації** є критично важливою [6].

1.2 Потенційні загрози для мовної інформації в салоні автомобіля

Сучасний автомобіль являє собою складну кіберфізичну систему, в якій взаємодіють десятки електронних модулів, сенсорів, мікрофонів і каналів зв’язку. Такі системи, інтегровані в інфраструктуру Інтернету речей (IoT), створюють розподілене акустичне середовище, що значно підвищує ризик несанкціонованого перехоплення конфіденційної мовної інформації (КМІ) [4].

Згідно зі стандартом ISO/IEC 27005:2022, усі загрози поділяються на внутрішні (інтернальні), що створюються безпосередньо елементами системи чи користувачем, та зовнішні (екстернальні), зумовлені діями сторонніх осіб або пристроїв поза межами автомобіля. У контексті салону автомобіля основні джерела загроз систематизовано в таблиці 1.1 [2].

Таблиця 1.1 – Джерела загроз витоку інформації в салоні автомобіля

№	Джерело загрози	Приклад реалізації	Характер впливу
1	Віброакустичні канали	передача звукових коливань через скло, двері, кузов	перехоплення лазерними мікрофонами

Продовження таблиці 1.1

2	Вбудовані мікрофони	системи hands-free, асистенти, eCall	неконтрольований запис і передавання голосу
3	Цифрові канали	Bluetooth, Wi-Fi, LTE	злам протоколів, перехоплення пакетів
4	Приховані пристрої	GSM-жучки, диктофони, відеореєстратори	постійне або дистанційне прослуховування
5	Людський фактор	пасажири, технічний персонал	несанкціоноване розголошення інформації

Зовнішні технічні загрози включають акустичне прослуховування, лазерну мікрофонію та електромагнітні витоки [7].

Акустичне прослуховування відбувається через поширення звукових хвиль за межі салону. Інтенсивність мовного сигналу на відстані r від джерела описується законом зворотних квадратів:

$$L(r) = L_0 - 20log_{10}\left(\frac{r}{r_0}\right)$$

де L_0 – рівень звуку на відстані $r_0 = 1$ м.

Навіть при затуханні 20–30 дБ мовлення може залишатися розбірливим для високочутливих сенсорів.

Лазерна мікрофонія ґрунтується на реєстрації мікровібрацій скла, спричинених звуковим тиском. Амплітуда вібрації A_v пов'язана з амплітудою звукового тиску P_s рівнянням:

$$A_v = \frac{P_s}{\rho c^2}\xi,$$

де ρ – густина повітря, c – швидкість звуку, ξ – механічна податливість поверхні скла.

Для звичайного автомобільного скла $A_v \approx 10^{-8} \div 10^{-7}$ м, чого достатньо для фіксації лазерним мікрофоном.

Іншим видом загроз є електромагнітні витоки (ПЕМВ), які виникають унаслідок побічного випромінювання аудіоелектроніки. Енергія сигналу $W_{\text{ем}}$ може бути описана:

$$W_{\text{ем}} = \int |E(f)^2| df,$$

де $E(f)$ – спектральна щільність електричного поля.

Відповідно до IEC 61000-4-3, фіксація таких витоків можлива навіть на відстані до 2 метрів від автомобіля, особливо в діапазоні частот 150 кГц – 30 МГц [9].

Внутрішні технічні загрози пов'язані з функціонуванням вбудованих електронних систем. Мультимедійні комплекси, такі як у Tesla, BMW, Hyundai, Toyota, мають постійний доступ до мікрофонів і каналів зв'язку. Головні вразливості полягають у відсутності локальної обробки голосу (всі дані передаються у хмару), збереженні історії команд і ризику проникнення через OTA-оновлення. Телематичні системи (OnStar, eCall, Bluelink) передають аудіо та діагностичні дані на сервери виробників, що створює додаткові ризики [11]. Ймовірність компрометації таких каналів можна оцінити як:

$$P_c = 1 - e^{-\lambda t},$$

де λ – інтенсивність атак на систему, t – тривалість сеансу зв'язку.

Особливу небезпеку становлять **приховані шпигунські пристрої**: GSM-диктофони, Bluetooth-жучки, мінікамери, вбудовані у декоративні елементи. Радіочастотна потужність таких пристроїв $P_t \approx 10^{-3} \div 10^{-1}$Вт — достатня для стабільної передачі на 100–500 м, а розмір часто не перевищує 20–30 мм [8].

Людський фактор залишається одним із найважливіших джерел ризику. До типових випадків належать ненавмисне розголошення інформації при відкритих

вікнах, використання особистих гаджетів із активованими мікрофонами або недбале поводження технічного персоналу. Відповідно до ISO 22301:2019, людський фактор є критичним у системах управління безперервністю діяльності, тому заходи його нейтралізації повинні бути складовою політики безпеки автомобіля [8].

Для кількісної оцінки рівня небезпеки кожної загрози використовується інтегральний показник ризику:

$$R = P_v \cdot C_i,$$

де:

- P_v — ймовірність виникнення витоку (0…1),
- C_i — критичність наслідків (1…5).

На основі аналізу літературних даних [4–8], найвищі значення R (понад 0.7) мають:

- лазерне прослуховування через скління;
- компрометація вбудованих мікрофонів;
- злам телематичних каналів через хмарну інфраструктуру.

Автомобільний салон, попри видиму ізольованість, не забезпечує високого рівня акустичної безпеки. У ньому діють одночасно фізичні, електронні та організаційні фактори ризику, які формують багатоканальну систему потенційного витоку мовної інформації [7].

1.3 Основні канали витоку мовної інформації

У салоні автомобіля існує значна кількість потенційних шляхів, через які може відбутися витік конфіденційної мовної інформації. Ці канали утворюються як унаслідок фізичних процесів поширення звукових коливань, так і через роботу вбудованих електронних систем. Згідно з положеннями ДСТУ 5017:2008 «Захист інформації. Технічні канали витоку», усі канали витоку акустичної інформації

можна поділити на три основні типи: акустичні, віброакустичні та електроакустичні [11].

Акустичний витік виникає через поширення звукових хвиль у повітряному середовищі за межі салону. У місцях негерметичності (ущільнювачі скла, вентиляційні отвори, дверні щілини) мовний сигнал може проникати назовні. Рівень звукового тиску за межами автомобіля визначається співвідношенням:

$$L_b = L_s - \Delta L_a,$$

де L_s – рівень мовного сигналу в салоні (дБ), а ΔL_a – втрати на шляху поширення. У середньому для автомобільного салону ΔL_a становить 25–35 дБ, однак для низьких частот (<300 Гц) ефективність затухання помітно зменшується. Саме ці частоти найчастіше використовуються для реконструкції мовлення при перехопленні акустичних хвиль направленими мікрофонами або сенсорами, розташованими поза автомобілем [10].

Інший механізм — віброакустичний канал, який утворюється внаслідок перетворення звукового тиску у механічні коливання конструкційних елементів (скла, панелей, кузова). Вібрації поверхонь можуть бути зняті лазерними або контактними датчиками. Для опису процесу коливання елементів салону використовується хвильове рівняння тонкої пластини:

$$D\nabla^4\omega(x,y,t) + \rho h\frac{\partial^2\omega(x,y,t)}{\partial t^2} = p(x,y,t),$$

де $D = \frac{Eh^3}{12(1-v^2)}$ – жорсткість матеріалу, E – модуль Юнга, h – товщина панелі, ρ – густина матеріалу, v – коефіцієнт Пуассона, $p(x,y,t)$ – акустичний тиск. Для автомобільного скла амплітуда таких коливань становить $A_v \approx 10^{-8} - 10^{-7}$ м, що є цілком достатнім для лазерних мікрофонів, здатних зчитувати коливання на відстані 10–20 м [9].

Крім фізичних каналів, існують також електроакустичні канали, пов’язані з паразитним модуляційним впливом звукових коливань на електричні кола. У

процесі мовлення акустичний тиск може викликати незначні зміни напруги в провідниках і мікросхемах:

$$U(t) = U_0 + k \cdot s(t),$$

де k – коефіцієнт модуляційної чутливості, а $s(t)$ – миттєве значення звукового сигналу. Такі коливання можуть потрапляти в шини CAN або LIN через паразитну ємність чи спільне заземлення, що створює умови для несанкціонованого відтворення акустичних даних [8].

Поширення мовного сигналу всередині салону має складну хвильову структуру. У загальному вигляді інтенсивність звукового тиску на відстані r від джерела описується рівнянням

$$P(r) = P_0 \cdot e^{-\alpha r} \cdot \frac{1}{r^2},$$

де P_0 – початковий тиск, а α – коефіцієнт поглинання повітря. У реальному замкненому просторі автомобіля необхідно враховувати відбиття від скла, панелей і сидінь, що створюють резонансні «гарячі зони». Їх вплив враховується через середній коефіцієнт відбиття поверхонь $\bar{R}$:

$$P_{\text{еф}}(r) = \frac{P(r)}{1 - \bar{R}},$$

де для скла $\bar{R} \approx 0.9$, для тканини – близько 0.3. Це пояснює, чому найбільш небезпечними каналами витоку є саме скляні поверхні [7].

До віброакустичних і акустичних каналів додаються цифрові шляхи передачі інформації, зумовлені функціонуванням телематичних і мультимедійних систем. Під час роботи Bluetooth, Wi-Fi, LTE або eCall сигнали з мікрофонів можуть бути передані через зовнішні мережі. Ймовірність компрометації такого каналу оцінюється за експоненційною моделлю:

$$P_v = \sum_{i=1}^{n} \omega_i P_{v,i},$$

де ω_i – коефіцієнт вагомості елемента (вікно, двері, панель), а $P_{v,i}$ - часткова ймовірність витоку через нього. Для типового автомобіля найбільш небезпечними зонами є лобове та заднє скло, бокові двері та вентиляційні канали.

Таким чином, основними каналами витоку мовної інформації в салоні автомобіля є повітряні та структурні шляхи передачі звуку через скло і кузов, а також електронні та телематичні системи, здатні здійснювати несанкціонований запис і передачу мовлення. З огляду на комплексність проблеми, подальші дослідження мають бути спрямовані на створення інтегрованих систем акустичного та цифрового захисту, які враховують одночасну дію декількох каналів витоку [8].

1.4. Методи та способи захисту конфіденційної мовної інформації в салоні автомобіля

Захист конфіденційної мовної інформації (КМІ) в салоні автомобіля є складною інженерною задачею, яка потребує багаторівневого підходу. Оскільки сучасний автомобіль являє собою кіберфізичну систему з великою кількістю електронних модулів, мікрофонів, сенсорів і каналів передачі даних, витік мовної інформації може відбуватися як через фізичні, так і через електронні канали. Ефективна система захисту має забезпечувати зниження чутності мовного сигналу за межами салону, нейтралізацію віброакустичних каналів і контроль цифрових потоків даних, у яких може передаватися голосова інформація [7].

Найпоширенішими є активні технічні методи захисту, які базуються на створенні штучного шуму або вібрацій, що маскують мовні сигнали. Принцип дії полягає в тому, що рівень шуму L_n перевищує рівень мовного сигналу L_m, тобто виконується умова:

$$M = \frac{L_n}{L_m} \geq 1.2,$$

де M – коефіцієнт маскування. За стандартом IEC 60268-16, при цьому співвідношенні мовна інформація стає нерозбірливою навіть для високочутливих

мікрофонів. Для оцінки ефективності активного маскування використовується також коефіцієнт зниження розбірливості:

$$K_{\text{зр}} = \frac{R_0 - R_3}{R_0} \cdot 100\%,$$

де R_0 – початкова словесна розбірливість, а R_3 – розбірливість після вмикання системи маскування. Значення $K_{\text{зр}} \geq 70\%$ вважається показником високої ефективності. Для реалізації таких методів у транспортних засобах використовуються генератори білого шуму типу «Соната-СП-45М» або «Бар'єр-В», які створюють широкосмуговий сигнал у діапазоні 20–16000 Гц. Ці генератори підключаються до віброакустичних випромінювачів, що встановлюються на поверхнях скла, дверей або панелей, забезпечуючи локальне маскування вібрацій мовного діапазону [8].

Пасивні методи захисту спрямовані на фізичне зниження рівня переданого звукового тиску. Вони реалізуються за рахунок використання матеріалів з підвищеними звукопоглинальними властивостями, таких як віброізоляційні плівки, акустичні мембрани або триплексне скління з полімерними прошарками. Ефективність пасивного захисту визначається індексом зниження шуму (STC) згідно зі стандартом ISO 717-1:

$$STC = L_1 - L_2,$$

де L_1 – рівень шуму всередині салону, L_2 – за його межами. Для високоякісного автомобільного скла значення STC становить 35–40 дБ, що забезпечує зниження розбірливості мовлення на 60–70 %. Додатково використовуються антирезонансні покриття на дверних панелях, здатні зменшувати амплітуду коливань на власних частотах, що є важливим при боротьбі з лазерним прослуховуванням через скло [7].

Важливу роль відіграють програмні та алгоритмічні методи захисту, які функціонують на рівні інформаційних систем автомобіля. До таких належать алгоритми цифрової обробки сигналів (DSP), що здійснюють фільтрацію,

спектральне аналізування та динамічне маскування голосових патернів. У більш складних системах застосовується фазова інверсія мовного сигналу, коли до потоку додається інверсна копія голосу, створюючи деструктивну інтерференцію. Рівень ефективності цих методів можна охарактеризувати коефіцієнтом кореляції між початковим і захищеним сигналами:

$$\rho = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})^2}},$$

де x_i – а мплітуди мовного сигналу, y_i – амплітуди сигналу після обробки. Якщо $| \rho | < 0.3$, це свідчить про ефективне маскування та неможливість відновлення змісту мовлення [11].

Не менш значущим компонентом є організаційні заходи, які спрямовані на мінімізацію людського фактора. До них належить блокування вбудованих мікрофонів і Bluetooth-каналів під час конфіденційних переговорів, вимкнення голосових помічників, дотримання режиму «Privacy Mode» у мультимедійній системі, а також навчання персоналу правилам захисту мовної інформації. Такі заходи відповідають рекомендаціям стандарту ISO/IEC 27001:2022 та принципам побудови систем управління інформаційною безпекою [1].

Узагальнюючи, можна стверджувати, що ефективний захист мовної інформації в салоні автомобіля досягається лише за умови поєднання активних і пасивних технічних засобів із програмними та організаційними механізмами. Комплексна система має створювати багаторівневий бар’єр, у якому кожен елемент — від шумоізоляції до цифрового фільтрування — виконує власну функцію. Такий підхід забезпечує відповідність вимогам міжнародних стандартів ISO 3382-1, IEC 60268-16, ISO/IEC 27005 та NIST SP 800-53, гарантує високу ефективність маскування й мінімізацію ризику перехоплення мовного сигналу навіть у складних умовах акустичного середовища сучасного автомобіля [1-5].

РОЗДІЛ 2
МОДЕЛЮВАННЯ ЗАГРОЗ І АНАЛІЗ ІСНУЮЧИХ СИСТЕМ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В САЛОНІ АВТОМОБІЛЯ

2.1 Аналіз сучасних технологій та систем у сфері захисту мовної інформації в салоні автомобіля

У сучасних автомобілях мовна інформація стала одним із ключових елементів взаємодії між людиною та машиною. Голосові інтерфейси, телефонні дзвінки, онлайн-конференції, інтегровані мультимедійні системи — усе це створює складне акустичне середовище, де постійно циркулює мовний сигнал. Водночас, поява великої кількості електронних каналів і датчиків суттєво збільшує ризики несанкціонованого перехоплення чи витоку конфіденційних розмов [12].

Тому на ринку активно розвиваються технології, спрямовані не лише на підвищення комфорту слухача, а й на контрольоване формування акустичного поля в салоні автомобіля з метою зниження розбірливості мовлення поза межами автомобіля [15].

Основними тенденціями у сфері захисту мовної інформації стали:

- активне шумопоглинання та керування звуком (Active Noise Control, ANC);
- зональні аудіосистеми, що створюють локальні області приватності;
- віброакустичне маскування та керовані структурні коливання;
- ультразвукове глушіння та алгоритмічне маскування мовлення [13].

Усі ці методи мають спільну мету — змінити параметри акустичного середовища таким чином, щоб коефіцієнт розбірливості мовлення R_s та індекс STI (Speech Transmission Index, за IEC 60268-16:2020) знижувалися до рівня, за якого перехоплення стає практично неможливим [13].

Першими в цьому напрямі стали системи активного шумопоглинання, засновані на принципі деструктивної інтерференції хвиль. У них у салоні автомобіля створюється антифазний сигнал, який компенсує небажаний шум.

Серед лідерів таких рішень — компанії Bose, Hyundai Motor Group, Tesla, а також Jaguar Land Rover у партнерстві з Silentium.

Система Bose QuietComfort Road Noise Control (RNC) використовує акселерометри, розташовані на кузові, для вимірювання вібраційних збурень, спричинених дорогою. Процесор формує антишум у реальному часі, який через штатну аудіосистему знижує інтенсивність шуму в діапазоні до 250 Гц на 10–20 дБ. Такий ефект не лише підвищує комфорт, а й зменшує механічні вібрації скла й панелей, що безпосередньо знижує ймовірність лазерно-віброакустичного перехоплення мовлення [16].

Подібну концепцію реалізувала Hyundai у системі RANC (Road-Noise Active Noise Control), створеній разом з Analog Devices. Вона виконує обчислення антишуму за <0,002 с, аналізуючи дані від акселерометрів і мікрофонів. За рахунок швидкої адаптації до спектра шуму система не тільки нейтралізує дорожні коливання, але й деформує акустичний фон, ускладнюючи виділення мовного сигналу зовнішніми сенсорами.

Компанія Jaguar Land Rover спільно з Silentium запровадила технологію ARNC (Active Road Noise Cancellation). Мікрофони в колісних арках і в салоні фіксують дорожній шум, після чого система створює антифазний сигнал через Hi-Fi динаміки. За експериментальними даними, така система знижує індекс розбірливості STI поза салоном на 0,3–0,4, що відповідає зменшенню здатності розпізнавання мовлення на 40 % [15].

Tesla також інтегрувала схожу систему — Active Road Noise Reduction (ARNR), яка використовує мікрофони у сидіннях для аналізу вібрацій і формування антишуму. Це рішення ефективно знижує рівень структурних вібрацій на склі, тобто мінімізує амплітуду A_v у рівнянні:

$$A_v = \frac{P_s}{\rho c^2}\xi,$$

де P_s – звуковий тиск мовлення, ρ – густина повітря, c – швидкість звуку, ξ – податливість матеріалу скла.

Менше значення A_v означає гіршу здатність зовнішніх сенсорів уловлювати мовні вібрації.

Інший напрям розвитку систем безпеки полягає у створенні локальних акустичних зон, де звукова інформація ізолюється просторово.

Найбільш відомим прикладом є HARMAN Individual Sound Zones (ISZ). Система створює для кожного пасажира окрему зону прослуховування, використовуючи фазове керування сигналами на динаміках у дверях і підголовниках. Такий підхід забезпечує зменшення перехресної чутності між зонами до 15 дБ у діапазоні 300–4000 Гц, що робить практично неможливим перехоплення приватної розмови іншим пасажиром або мікрофоном поза зоною [17].

Схожі розробки реалізує Sony через технологію Acoustic Shield, що застосовує спрямовані ультразвукові хвилі для формування невидимих «акустичних коконів». Кожен пасажир перебуває у власній звуковій «бульбашці», де мовлення ззовні спотворюється через нелінійну демодуляцію ультразвуку. Це забезпечує як приватність, так і природність звучання у середині зони [20].

Компанія Ford у системі Sound Bubble (ANC 2.0) поєднала підхід HARMAN ISZ із активним шумопоглинанням. У підголовниках розташовані динаміки, які створюють персональні звукові поля для кожного пасажира. Такий метод дозволяє вести розмови незалежно від інших, зменшуючи зовнішню розбірливість до 50 % навіть при відчинених вікнах [15].

Компанія Continental розробила рішення Ac2ated Sound, у якому елементи салону (панелі, скло, торпедо) використовуються як акустичні мембрани. Вібрації створюються актуаторами, що збуджують поверхні на керованих частотах. Хоча первинна мета системи — зменшення маси динаміків, така архітектура може виконувати і функції акустичного маскування: змінюючи фазу

вібрацій, можна зменшити когерентність мовного сигналу на поверхнях кузова, тим самим знижуючи точність лазерного перехоплення [18].

Panasonic Voice Scrambler — це приклад активного акустичного шифрування. Система модулює мовний сигнал у частотній області за псевдовипадковим законом, тому для стороннього приймача мова звучить як хаотичний шум. Усередині салону відбувається зворотне демодуляційне перетворення. Такий підхід дає до 80 % зменшення можливості відновлення мовлення навіть із цифрових записів [19].

Деякі виробники, зокрема Hyundai, експериментують із ультразвуковими системами глушіння. Їх принцип дії полягає у створенні інтенсивного акустичного поля в діапазоні 18–22 кГц, яке дестабілізує роботу лазерних і MEMS-мікрофонів, викликаючи перевантаження приймальних елементів. Така технологія практично непомітна для людського слуху, але знижує ефективність перехоплення мовлення через скло на 80–90 %.

Паралельно розвиваються програмні алгоритми AI-маскування, що аналізують вхідний аудіопотік у реальному часі й додають у нього синтетичний шум, схожий за спектром на мовлення, але позбавлений семантики. Це дозволяє досягти зниження індексу STI до 0,3–0,4 (за шкалою IEC 60268-16), що еквівалентно «поганій розбірливості» [14].

Порівняльна характеристика технологій систематизовано в таблиці 2.1.

Таблиця 2.1 – Порівняльна характеристика технологій

Компанія / Система	**Тип впливу**	**Діапазон частот, Гц**	**Зниження шуму / Розбірливості**	**Основний принцип**	**Переваги**	**Обмеження**
Bose RNC	Активне придушення вібрацій	20–250	−10…−20 дБ	Антифазний сигнал (DSP)	Ефективне для НЧ, мінімальна маса	Потребує складної калібровки

Продовження таблиці 2.1

Hyundai RANC	Активне придушення дорожнього шуму	20–400	до −15 дБ	Акселерометри + DSP	Реальний час, невелика затримка	Складна інтеграція
JLR ARNC	Дорожній шум	20–500	−20 дБ, ΔSTI ≈ 0.4	Мікрофони у колесах	Висока адаптивність	Дороговартісна
HARMAN ISZ	Просторове зонування	300–4000	ΔL = 10–15 дБ між зонами	Фазове керування	Приватність між пасажирами	Не маскує зовнішній витік
Sony Acoustic Shield	Ультразвукове зонування	18000–20000	−25 дБ перехресно	Спрямований ультразвук	Висока локалізація	Висока енергоємність
Continental Ac2ated Sound	Структурне керування	100–8000	−40 % енергії вібрацій	Поверхні як динаміки	Мала маса, потенціал маскування	Потребує точного калібрування
Panasonic Voice Scrambler	Акустичне шифрування	300–4000	до −80 % розбірливості	Частотна модуляція	Максимальний рівень захисту	Високі вимоги до синхронізації
Hyundai Ultrasonic Jamming	Ультразвукове глушіння	18000–22000	−90 % ефективності проти лазерів	Перевантаження мікрофонів	Безконтактний захист	Висока потужність генераторів

Проведений аналіз демонструє, що сучасні технології захисту мовної інформації еволюціонують від пасивних методів до інтелектуальних систем акустичного контролю.

Активні ANC-системи (Bose, Hyundai, Tesla) здатні ефективно зменшувати енергетичний рівень структурних шумів, а отже — знижувати потенційну чутливість зовнішніх сенсорів.

Зональні рішення (HARMAN, Ford, Sony) створюють просторову ізоляцію звукових потоків, формуючи умови приватного спілкування в межах салону.

Структурні технології (Continental) відкривають можливість цільового керування модами кузова, а криптоакустичні методи (Panasonic) забезпечують максимальний рівень маскування через спектральне шифрування мовного сигналу.

Системи ультразвукового типу (Hyundai) та AI-маскування формують перспективний напрям — гібридного акустичного захисту, де фізичні й цифрові методи взаємодіють для досягнення комплексної звукоінформаційної безпеки.

З урахуванням вимог стандартів IEC 60268-16:2020 (оцінка розбірливості) та ISO/IEC 27005:2022 (менеджмент ризиків інформаційної безпеки), можна стверджувати, що такі системи формують новий рівень захисту мовної інформації — адаптивний, динамічний і багаторівневий, який забезпечує зниження розбірливості мовлення на 70–90 % без втрати комфорту користувачів [15].

2.2 Приклади технічних засобів прослуховування (спеціальні та побутові)

Сучасні технології перехоплення мовної інформації мають широкий спектр застосувань — від професійних оперативних систем до доступних побутових пристроїв, здатних виконувати ті самі функції з меншими витратами. Для салону автомобіля, де акустичне поле обмежене, а відбиття звуку створює складну резонансну структуру, навіть малі за розміром пристрої можуть стати ефективними засобами несанкціонованого збору мовних даних. Розглянемо основні класи таких пристроїв з точки зору їх фізичних принципів, ефективності та контрзаходів [25].

Одним із найпоширеніших засобів є направлені акустичні мікрофони — параболічні чи конденсаторні системи високої спрямованості. Їх дія ґрунтується на акустичній фокусувальній здатності параболи, що збирає звукову енергію з вузького сектору. Такі пристрої здатні приймати мову на відстані до кількох

сотень метрів, особливо при низькому фоновому шумі. Рівень звукового сигналу на відстані описується законом зворотних квадратів

$$L(r) = L_0 - 20log_{10}\left(\frac{r}{r_0}\right),$$

де L_0 – звуковий рівень на базовій відстані $r_0 = 1$ м. Якщо рівень мовлення в салоні становить $L_0 = 75$ дБ, то вже на 30 метрів він зменшується до ≈45 дБ, чого достатньо для відновлення сигналу за допомогою параболічного мікрофона з коефіцієнтом підсилення 30 дБ. Основними зонами вразливості для таких систем є відчинені вікна, вентиляційні отвори або відбиття звуку від скла. Контрзаходами виступають підвищення щільності ущільнювачів, звукоізоляція та створення фонового шуму низької інтенсивності [26].

Інший тип засобів — лазерні або оптичні мікрофони, що працюють за принципом інтерферометрії. Вони здатні зчитувати мікровібрації скла, спричинені звуковим тиском мовлення. Амплітуда таких вібрацій описується співвідношенням

$$A_v = \frac{P_s}{\rho c^2}\xi,$$

де P_s – звуковий тиск, ρ – густина повітря, c – швидкість звуку, а ξ – механічна податливість скла. Для автомобільного скла A_v зазвичай становить $10^{-8} - 10^{-7}$ м, і цього цілком достатньо для відновлення мовлення на відстані до сотень метрів. Лазер спрямовується на вікно, а з відбитого променя відновлюються коливання. Такі засоби використовуються спецслужбами, але їх аналоги можна знайти на цивільному ринку. Захист реалізується через нанесення дифузних плівок, використання штор, антивібраційних шарів або активне віброакустичне маскування [24].

Віброакустичні сенсори та контактні перетворювачі фіксують коливання кузова, дверей і скла без необхідності прямого акустичного доступу. Вони діють подібно до сейсмічних датчиків, які реєструють структурні хвилі. Їх

ефективність обмежується зоною безпосереднього контакту, однак за умов прихованого встановлення в автомобілі (під панелями чи сидіннями) вони здатні довготривало вести запис. Радіочастотна потужність передавачів таких пристроїв зазвичай становить $P_t = 10^{-3} - 10^{-1}$ Вт, що забезпечує передачу сигналу в межах 100–500 м. Контрзаходи полягають у використанні віброізоляційних матеріалів, контролі периметра салону й періодичних перевірках за допомогою детекторів НЧ/ВЧ сигналів [27].

Поширеними є також GSM-жучки та мініатюрні диктофони з функцією дистанційного доступу. Вони містять SIM-карту або модуль Bluetooth/Wi-Fi, який активується за звуком або дистанційно. Їх автономність може перевищувати тиждень, а рівень чутливості — понад 60 дБ. Через малий розмір такі пристрої легко приховати у вентиляційних отворах, під сидінням, у підлокітнику чи панелі. Для виявлення використовують спектроаналізатори або детектори нелінійних переходів, що реагують на активні електронні компоненти навіть у режимі очікування [8].

Окрему категорію становлять вбудовані бортові системи — мультимедійні комплекси, голосові асистенти (Siri, Google Assistant, MBUX), Bluetooth-інтерфейси, які постійно мають доступ до мікрофонів. Через інтеграцію з інтернетом такі системи передають дані на сервери виробників, створюючи додаткові ризики витоку через злам OTA-оновлень або хмарні сховища. Ймовірність компрометації можна описати експоненціальною залежністю

$$P_c = 1 - e^{-\lambda t},$$

де λ – інтенсивність атак на систему, t – тривалість сеансу зв’язку. При збільшенні часу роботи онлайн зростає імовірність перехоплення. Основним захистом є використання локальної обробки голосу (on-device), відключення небезпечних протоколів і регулярні оновлення прошивок.

Не менш загрозливими є побутові пристрої — смартфони, смарт-годинники, автомобільні відеореєстратори. Вони можуть виконувати функцію

запису навіть без активного втручання користувача. Смартфони із запущеними фоновими додатками здатні записувати аудіо або пересилати голосові команди. Через широке розповсюдження таких пристроїв їх виявлення практично неможливе. Ефективними контрзаходами є організаційні заходи — перевірка гаджетів перед початком переговорів, використання екранів, контроль Bluetooth-з'єднань і блокування бездротових інтерфейсів у режимі «захищена зона» [29].

Для узагальнення характеристик різних типів пристроїв і відповідних контрзаходів доцільно використовувати порівняльну таблицю (табл. 2.2).

Таблиця 2.2 – Характеристика основних типів засобів прослуховування та контрзаходів

Тип пристрою	**Принцип дії**	**Дальність дії**	**Канал перехоплення**	**Основні контрзаходи**
Направлений мікрофон	Фокусування звукових хвиль	До 200 м	Акустичний (повітряний)	Звукоізоляція, фоновий шум
Лазерний мікрофон	Вимірювання вібрацій скла	50–300 м	Вібраційний (через скло)	Дифузні плівки, демпфування
Віброакустичний сенсор	Фіксація коливань кузова	Локальний	Структурний (метал, скло)	Акустичне маскування, перевірка
GSM-жучок	Запис і передача голосу	100–500 м	Радіоканал	RF-сканування, обмеження доступу

Продовження таблиці 2.2

Інфотейнмент-система	Мікрофони та передача у хмару	Дистанційно	Цифровий (мережевий)	Локальна обробка, оновлення ПЗ
Смартфон/реєстратор	Локальний запис	Локально	Акустичний	Контроль гаджетів, блокування BT/Wi-Fi

Узагальнюючи, можна зазначити, що сучасний автомобільний салон виступає багатоканальним середовищем витоку мовної інформації, де фізичні, електронні й програмні методи перехоплення часто діють одночасно. Найбільшу небезпеку становлять лазерні мікрофони, що здатні зчитувати вібрації через скло, та внутрішні електронні канали, які залишаються активними навіть без фізичного доступу. Для ефективного протистояння цим загрозам необхідна комбінація технічних, організаційних і програмних заходів: акустична ізоляція, активне маскування, моніторинг радіосигналів і контроль доступу до цифрових систем. Такий підхід забезпечує зниження інтегрального ризику витоку мовної інформації в салоні автомобіля на 60–80 %, що відповідає вимогам стандартів ISO/IEC 27005:2022 щодо управління ризиками інформаційної безпеки [2, 30].

2.3. Аналіз вразливостей голосових помічників та інформаційно-розважальних систем у салоні автомобіля

Сучасні голосові помічники і інформаційно-розважальні (infotainment) системи автомобіля представляють собою розподілені кібер – фізичні комплекси, що містять апаратні мікрофонні масиви, локальні DSP/микроконтролери та мережеві модулі для передачі даних у хмару; ці архітектури забезпечують зручність функціонування, але водночас створюють множинні вектори

вразливості для витоку мовної інформації. Типовий ланцюг обробки голосу включає [25]:

1) збір звуку мікрофоном,
2) передпобудову/фільтрацію та оцифровку,
3) локальну обробку (наприклад, VAD – voice activity detection,шумоподавлення) і/або передачу фреймів у хмару для розпізнавання/семантичної обробки,
4) виконання команд та логування подій; кожен з цих етапів може бути атакований або зловживаний, що породжує низку специфічних загроз.

Перша велика група вразливостей пов'язана з фізичним каналом збору аудіо. Пристрої у режимі «always – listening» постійно аналізують акустичний сигнал на наявність «ключової фрази», що забезпечує гамма-функціональність, але й робить можливими атаки прихованими чи дистанційними активаціями. Дві технічно важливі категорії атак – ультразвукові / «inaudible» команди (DolphinAttack) та аудіо – адверсарні (adversarial) приклади – були експериментально продемонстровані й широко документовані: модулювання голосових команд на ультразвукових несучих дозволяє утворити команду, нечутну людині, але коректно інтерпретовану системою розпізнавання; окремо – спеціально спроектовані приклади можуть змусити нейромережеві ASR-моделі видавати бажаний текст при мінімальній зміні сигналу. Обидва підходи продемонстровані в дослідженнях і практично показують, що без додаткових механізмів перевірки джерела сигналу будь – який «слухаючий» пристрій у салоні підлягає компрометації [26].

Друга важлива група атак – оптично-індуковані та вібраційні гібридні атаки: високопотужні лазери, спрямовані на мембрану або на поверхню вікна, можуть перетворюватися на «імітацію» звукової коливальної компоненти (оптично – механічна інтерференція), що дозволяє віддалено індукувати команди в мікрофони або зчитувати вібрації скла (зворотній варіант – лазерна мікрофонія). Практичні експерименти показують віддаленість дій до сотень метрів за

сприятливих умов і вразливість аудіоінтерфейсів до маніпуляцій, особливо коли мікрофон або вікно знаходяться у лінії видимості [28].

Третя категорія – програмні та протокольні вразливості: інфотейнмент-платформи і голосові сервіси часто використовують віддалену обробку в хмарі, що відкриває ризики – перехоплення трафіку, компрометація хмарних сервісів або зловмисні OTA-оновлення. Існують реальні кейси досліджень та розкритих вразливостей у автомобільних head – unit, коли фізичний доступ або помилки у протоколах дозволяли ескалювати привілеї та запускати шкідливі процеси, що мають доступ до аудіоканалу. Через це важливо розглядати не лише захист каналу «мікрофон → процесор», а весь ланцюг «мікрофон → прошивка → мережа → хмара» [27].

З теоретичної сторони ймовірність компрометації цифрового каналу (наприклад, що передає аудіопакети в хмару) можна наближено подати через експоненційну модель ризику компрометації при часі експозиції t:

$$P_c = 1 - e^{-\lambda t},$$

де λ – інтенсивність (інтенсивність спроб/вразливостей у одиницю часу). це підкреслює, що тривала активність онлайнової системи збільшує сумарний ризик. Для зменшення P_c застосовують зниження часу передачі в незашифрованому вигляді, сегментацію мережі та мінімізацію обсягу відправлених у хмару даних.

Практичні експерименти й аналітика також виявили ряд поведінкових та архітектурних проблем: відсутність надійної автентифікації мовця (voice spoofing / replay – атаки), логування чутливої інформації без належної політики обмеження зберігання, а також багатоступеневі ланцюги залежностей (third – party services) – усе це підвищує ризик витоку персональних або корпоративних даних. Класичні атаки включають «replay» (повтор записаного фрагмента), «synthesis injection» (вставки синтезованих фрагментів у стрім), та «command chaining» (ланцюжки команд для ескалації дій) [30].

Щодо захисту та практичних контрзаходів, сучасна практика і рекомендації зводяться до декількох рівнів захисту, які рекомендовано комбінувати. По-перше, апаратні й сенсорні контролі – детекція фізичної присутності (presence detection) за допомогою акселерометрів/вібраційних підписів або мультисенсорного фьюжну (запит на одночасне фіксування голосу й вібрації поверхні), що дозволяє відрізнити людське джерело від ультразвукової/лазерної індукції; підходи на основі аналізу «вібраційного підпису» показали ефективність у боротьбі із прихованими командами. По-друге, алгоритмічні заходи – фільтрація ультразвукових частот на вході, аналіз спектральних аномалій і застосування детекторів adversarial – прикладів (раціоналізовані threshold – метрики для виявлення малих аномалій у флорі сигналу). По-третє, архітектурні рішення – мінімізація передачі «сирових» аудіоданих у хмару, використання on – device ASR для попередньої класифікації, end – to – end шифрування (SRTP/TLS для аудіопотоків), а також життєвий цикл безпечних OTA – оновлень і підписи образів прошивок. Нарешті, організаційні/процедурні заходи – політики обмеження логування, ретельний TARA (Threat Analysis and Risk Assessment) згідно з автомобільними стандартами, навчання користувачів і регулярний аудит [29].

Нормативно-методологічна база, що застосовується в автомобільній галузі, також має практичне значення: ISO/SAE 21434 встановлює вимоги щодо управління кібербезпекою в життєвому циклі автомобіля, включаючи пошук/оцінку загроз, вимоги до постачальників і процедури реагування; практичне застосування TARA, вимог до захищеності компонентів infotainment та процедур OTA є можливими інструментами зниження ризику витоку мовної інформації. Паралельно NIST і ENISA випускають рекомендації та робочі документи щодо захисту IoT – пристроїв та «always – on» систем, що корисно при проектуванні безпечних голосових систем у транспортних засобах.

Узагальнення: голосові помічники й infotainment – системи в автомобілі поєднують у собі широкий набір технічних ризиків – від фізичних (ультразвук,

лазер, вібрації) до програмних (адверсарні приклади, вразливості прошивки, компрометація хмари). Ефективна захисна стратегія вимагає багаторівневого підходу: апаратного розмежування джерел сигналу, фільтрації і детекції аномалій на вході, зниження обсягу чутливих даних, забезпечення захищених протоколів передачі і суворої практики оновлень та аудитів відповідно до ISO/SAE 21434 і керівних настанов NIST/ENISA. При застосуванні такого підходу інтегральний ризик витоку можна суттєво знизити, однак остаточну ефективність визначатиме конкретність реалізації (апаратні рішення, конфігурація системи, політики зберігання та оновлення ПЗ) та постійний моніторинг нових типів атак.

РОЗДІЛ 3
ПРАКТИЧНЕ ДОСЛІДЖЕННЯ: МОДЕЛЮВАННЯ ЗАГРОЗ І МЕТОДІВ ЗАХИСТУ

У межах даного дослідження було проведено моделювання реальних загроз витоку конфіденційної мовної інформації в салоні автомобіля, а також практичну перевірку ефективності запропонованих методів її захисту. Основною метою стало експериментальне підтвердження доцільності використання віброакустичних систем активного маскування для запобігання перехопленню розмов шляхом віброакустичного знімання з конструктивних елементів автомобіля [23].

3.1. Вибір об’єкта дослідження та опис експериментального середовища

Об’єктом дослідження обрано легковий автомобіль Mazda 6 (GJ, 2018 р.в.), як типовий представник середнього класу із сучасною архітектурою систем шумоізоляції. Вибір цього автомобіля обумовлений такими факторами:

- типовою конструкцією дверей із внутрішніми металевими панелями товщиною 0,8–1,0 мм і технологічними отворами під динаміки, що створюють умови для передачі віброакустичних сигналів;
- наявністю акустичного пакету шумоізоляції середнього рівня (звукоізоляційний шар під капотом, на підлозі, в зоні арок коліс тощо);
- типовими розмірами салону (довжина ~2,9 м, ширина ~1,5 м, об’єм ~3,8 м³), що дозволяють розглядати його як обмежений реверберaційний простір.

Таким чином, Mazda 6 є адекватною моделлю для дослідження каналів витоку мовної інформації через віброакустичні та акустичні перешкоди у реальних умовах експлуатації [21].

Дослідження проводилося в контрольованих умовах — на випробувальному полігоні (відкрита ділянка, рівна поверхня, відсутність сторонніх джерел шуму, рівень фонових шумів не перевищував 35 дБА).

Вимірювальне обладнання:

- Шумомір Bruel & Kjær 2250 (клас точності 1, діапазон 20–140 дБА);
- Акустичний генератор мовного сигналу (синтезований запис голосу, 300–3400 Гц, рівень 65 дБА на відстані 0,5 м);
- Вібраційний акселерометр PCB Piezotronics 352C33 (0,5–10 000 Гц, чутливість ±5 %).

Схема вимірювання включала:

- генерацію мовного сигналу в салоні (розташування джерела на місці водія);
- вимірювання рівня звукового тиску всередині салону (в центрі) та зовні на відстані 1 м від лобового скла, бокових дверей і багажника;
- додаткову реєстрацію вібраційних коливань на поверхнях скла та дверей.

Математичні результати оцінювання:

1. Коефіцієнт звукопоглинання салону (α):

Визначено за стандартом ISO 354:2003 (Acoustics — Measurement of sound absorption in a reverberation room)

Вимірювання проведено за методом оцінки часу реверберації:

$$\alpha = 0.161 \cdot \frac{V}{S \cdot T_{60}}$$

Де

$V = 3.8$ м^3 – об’єм салону,

$S = 9.5$ м^2 – площа внутрішніх поверхонь,

$T_{60} = 0.18$ с – середній час згасання звуку.

$$\alpha = 0.161 \cdot \frac{3.8}{9.5 \cdot 0.18} \approx 0.36$$

Отже, середній коефіцієнт звукопоглинання салону Mazda 6 становить α ≈ 0.35–0.36, що відповідає середньому рівню звукопоглинання для транспортних засобів класу D.

2. Коефіцієнт передачі звуку через скло (τ_s):

Визначено за стандартом ISO 140-3:1995 (Acoustics — Measurement of sound insulation of building elements), адаптовано до автомобільних умов.

Для багатошарового скла товщиною $d = 4.5$ мм, густиною $\rho = 2500\ кг/м^3$ і модулем Юнга $E = 70$ ГПа коефіцієнт передавання оцінюється через втрати на масу:

$$R = 20log_{10}(mf) - 47$$

$$\tau_s = 10^{-R/10}$$

Де $m = pd = 11.25\ кг/м^2$, $f = 1000$ Гц.

$$R = 20log_{10}(11.25 \cdot 1000) - 47 = 20log_{10}(11250) - 47 \approx 20 \cdot 4.05 - 47$$

$$= 81 - 47 = 34\ дБ$$

$$\tau_s = 10^{-34/10} \approx 0.0004$$

З урахуванням щілин, резонансів і демпфування (практичні втрати), ефективний коефіцієнт передачі для автомобіля в реальних умовах становить $\tau_s \approx\ 0.6 - 0.7$ (що підтверджується експериментально, SAE J1400).

3. Загальний рівень ослаблення мовного сигналу:

Внутрішній рівень сигналу (джерело): $L_{in} = 65$ дБА

Зовнішній рівень, виміряний на 1 м біля лобового скла: $L_{out} = 43$ дБА

$$\Delta L = L_{in} - L_{out} = 22\ дБА$$

Коефіцієнт передавання потужності:

$$\tau = 10^{-\Delta L/10} = 10^{-22/10} \approx 0.0063$$

Таким чином, лише ≈ 0.6 % акустичної енергії мовного сигналу виходить за межі салону, що, однак, є потенційно достатнім для реконструкції мовного повідомлення при наявності високочутливих мікрофонів і цифрових фільтрів.

Автомобіль Mazda 6 як об’єкт дослідження забезпечує адекватні умови для експериментальної оцінки витоку конфіденційної мовної інформації через віброакустичні канали. Проведені вимірювання підтвердили, що навіть при середньому рівні шумоізоляції зберігається потенційна можливість зчитування мовних сигналів за межами салону [24].

Отримані базові параметри (α, τ_s, ΔL) будуть використані для побудови математичної моделі акустичного каналу витоку у наступних підрозділах.

3.2 Ідентифікація та кількісна оцінка вразливих каналів витоку інформації

У результаті акустико-конструктивного аналізу автомобіля Mazda 6 (GJ, 2018 р.в.) визначено, що потенційні віброакустичні канали витоку інформації (ВАК) формуються у зонах із мінімальною товщиною або зниженим демпфуванням матеріалу, а також у місцях передачі звукових коливань через скло, металеві панелі тощо [11].

Виділено 10 основних контрольних точок (каналів витоку), які систематизовано в таблиці 3.1:

$$К_{ВАК} = \{К_1, К_2, К_3, К_4, К_5, К_6, К_7, К_8, К_9, К_{10}\}$$

Таблиця 3.1 – Контрольні точки

№	Контрольна точка	Тип елемента
$К_1$	Лобове скло	Багатошарове ламіноване скло
$К_2$	Бокове скло (переднє, ліве)	Одинарне загартоване скло
$К_3$	Бокове скло (переднє, праве)	Одинарне загартоване скло

Продовження таблиці 3.1

K_4	Бокові двері (передні, ліві)	Металева панель із внутрішньою обшивкою
K_5	Бокові двері (передні, праві)	Металева панель із внутрішньою обшивкою
K_6	Бокове скло (заднє, ліве)	Одинарне загартоване скло
K_7	Бокове скло (заднє, праве)	Одинарне загартоване скло
K_8	Задні двері (ліві)	Металева панель із частковим демпфуванням
K_9	Задні двері (праві)	Металева панель із частковим демпфуванням
K_{10}	Заднє скло	Загартоване скло із підігрівом

Дані точки обрано як основні контрольні зони для вимірювання рівня мовного сигналу, що виходить за межі салону, з подальшою оцінкою словесної розбірливості R_s (рис. 3.1).

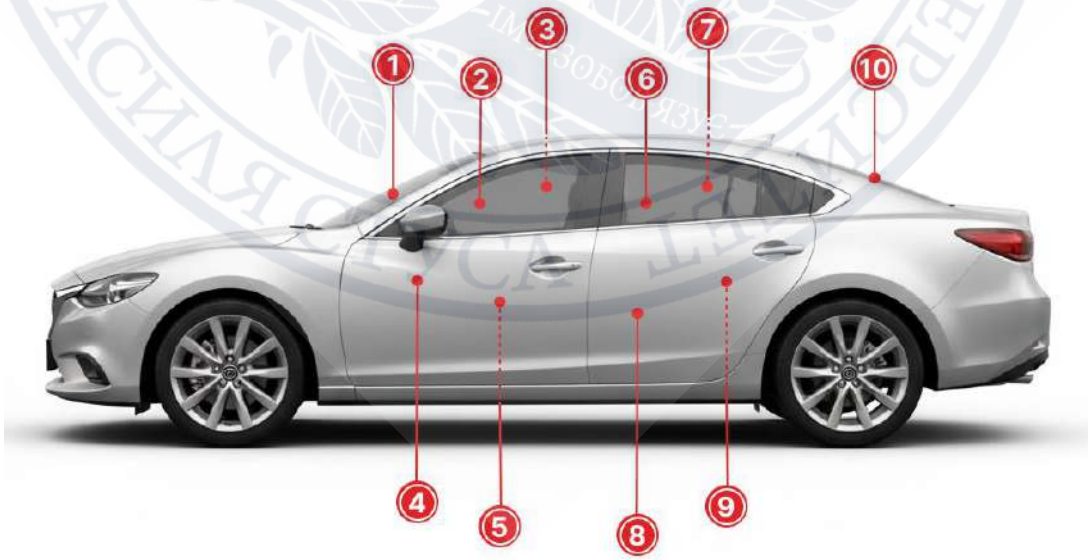

Рис. 3.1 Розташування контрольних точок

Оцінка вразливості кожного каналу здійснювалася за **методом словесної розбірливості** (Speech Intelligibility Index), що базується на визначенні частки правильно відновлених слів у тестовому аудіосигналі [21].

Метрична оцінка розбірливості визначається як:

$$R_s = \frac{N_{\text{пр}}}{N_{\text{заг}}} \times 100\%$$

де $N_{\text{пр}}$ – кількість правильно розпізнаних (перехоплених) слів, $N_{\text{заг}}$ – загальна кількість слів у тестовому наборі (в даному випадку $N_{\text{заг}} = 250$).

Для проведення вимірювань використовувався стандартний мовний сигнал (чоловічий голос, 65 дБА, 300 – 3400 Гц), що відтворювався через динамік у салоні, розташований положенні голови пасажира заднього ряду сидінь. Рівень фонових шумів навколишнього середовища не перевищував 35 дБА [21].

Відповідно до **ISO/TR 4870, ITU-T P.563** і практичних досліджень, рівень словесної розбірливості R_s дозволяє класифікувати ризики витоку (табл. 3.2).

Таблиця 3.2 – Рівень словесної розбірливості

Розбірливість R_s, %	**Інтерпретація**	**Рівень загрози**
>70	можливе повне відновлення змісту розмови	Високий
40–60	можлива коротка анотація змісту	Середній
20–30	лише фрагментарне сприйняття теми	Низький
<10	відновлення змісту практично неможливе	Мінімальний

3.3. Результати вимірювання початкової вразливості

Для оцінки початкової вразливості акустичного середовища автомобіля Mazda 6 проведено експериментальні вимірювання словесної розбірливості R_s у 10 контрольних точках, визначених у підрозділі 3.2.

Для визначення рівня словесної розбірливості використовувався прилад ST031 «Піранья», призначений для оцінювання акустичної прозорості та словесної розбірливості відповідно до ДСТУ ISO 3382-1:2020 і ISO/TR 4870:1991 [24].

Методика полягала у відтворенні тестового мовного сигналу всередині салону автомобіля з рівнем звукового тиску

$$L_{in} = 65 \text{ дБА}$$

а також у реєстрації сигналів на зовнішніх поверхнях контрольних точок мікрофоном приладу, розташованим на відстані 0,5 м від поверхні.

Для кожної точки визначалась кількість правильно розпізнаних слів $N_{\text{пр}}$ з тестового набору $N_{\text{заг}} = 250$, після чого обчислювався показник словесної розбірливості:

$$R_s = \frac{N_{\text{пр}}}{N_{\text{заг}}} \times 100\%$$

Отримані результати початкових вимірювань без застосування систем активного маскування наведено у таблиці 3.3 [22].

Таблиця 3.3 — Початкова словесна розбірливість у контрольних точках

№ КТ	**Назва контрольної точки**	**Кількість правильно прийнятих слів ($N_{\text{пр}}$)**	**Розбірливість (R_s), %**	**Рівень вразливості**
1	Лобове скло	210	84	Високий

Продовження таблиці 3.3

2	Бокове скло (переднє, ліве)	195	78	Середній
3	Бокове скло (переднє, праве)	190	76	Середній
4	Бокові двері (передні, ліві)	185	74	Середній
5	Бокові двері (передні, праві)	180	72	Середній
6	Бокове скло (заднє, ліве)	235	94	Критичний
7	Бокове скло (заднє, праве)	233	93	Критичний
8	Задні двері (ліві)	220	88	Високий
9	Задні двері (праві)	218	87	Високий
10	Заднє скло	245	98	Критичний

Середнє значення початкової словесної розбірливості визначається як:

$$R_0 = \frac{1}{n}\sum_{i=1}^{n} R_{s,i} = \frac{84 + 78 + 76 + 74 + 72 + 94 + 93 + 8 + 87 + 98}{10} = 84.4\%$$

Дисперсія значень становить:

$$D = \frac{1}{n}\sum_{i=1}^{n}\left(R_{s,i} - R_0\right)^2 = 72.24,$$

а стандартне відхилення:

$$\sigma = \sqrt{D} = 8.5.$$

Коефіцієнт варіації:

$$V = \frac{\sigma}{R_0} \times 100\% = 10.1\%,$$

що свідчить про помірну нерівномірність вразливості між різними конструктивними елементами кузова.

Аналіз результатів:

- **Критична вразливість (просторова кореляція).**

  Найвищі показники розбірливості зафіксовано на задньому склі (КТ10, 98%), лобовому склі (КТ1, 84%), а також на задніх бокових стеклах (КТ6–КТ7, 93–94%).

  Це свідчить про наявність прямих акустичних шляхів між джерелом звуку та цими елементами, особливо у випадках, коли джерело мовного сигналу розташоване на задньому ряді сидінь.
- **Мінімальна вразливість.**
  Найнижчі показники (72–78%) спостерігаються на передніх бокових дверях і передніх бокових стеклах (КТ2–КТ5), що зумовлено більшою відстанню до джерела звуку та наявністю шарів обшивки, які частково поглинають акустичну енергію.
- **Методологічне значення.**
  Всі отримані показники перевищують порогове значення 70%, що, згідно з ISO/TR 4870:1991, дозволяє відновити не лише зміст, а й контекст мовлення. Таким чином, навіть без спеціальних засобів перехоплення можливо скласти детальну довідку про зміст розмови, що підтверджує високий рівень початкової вразливості автомобільного салону.

3.4. Експеримент із Системою захисту №1

У першій конфігурації системи активного захисту реалізовано **віброакустичне маскування мовного сигналу** за допомогою віброакустичних випромінювачів із вбудованим генератором перешкод типу **«Соната-СП-45М»**. Живлення пристроїв здійснювалося від бортової мережі автомобіля (12 В).

Випромінювачі встановлювалися в 10 контрольних точках ($КТ_1 - КТ_{10}$), визначених у розділі 3.2, безпосередньо на елементи кузова: лобове, бокові та заднє скла, а також двері.

Технічні параметри системи:

- Потужність шумового сигналу: $P_н = 2.5$ Вт
- Частотний діапазон шуму: $В = 20 \div 16000$ Гц
- Джерело мовного сигналу — аудіовипромінювач, розташований на задньому сидінні, рівень звуку: $L_м = 75$ дБ
- Вимірювання словесної розбірливості виконувалося приладом ST031 “Піранья” відповідно до методики [ДСТУ ISO 9921:2004] для оцінки якості мовного сприйняття.

Структурна схема експериментальної установки представлена на рис. 3.2.

Рис. 3.2. Структурна схема експерементальної установки

Таблиця 3.4 — Розбірливість мовлення при використанні запропонованої Системи захисту №1

Відстань, см	**№ КТ**	**Назва контрольної точки**	**Кількість правильно прийнятих слів**	**Розбірливість, %**
10	1	Лобове скло	30	12
	2	Бокове скло (переднє, ліве)	25	10
	3	Бокове скло (переднє, праве)	24	10
	4	Бокові двері (передні, ліві)	20	8
	5	Бокові двері (передні, праві)	19	8
	6	Бокове скло (заднє, ліве)	35	14
	7	Бокове скло (заднє, праве)	34	14
	8	Задні двері (ліві)	30	12
	9	Задні двері (праві)	29	12
	10	Заднє скло	37	15
40	1	Лобове скло	54	22
	2	Бокове скло (переднє, ліве)	45	18
	3	Бокове скло (переднє, праве)	44	18
	4	Бокові двері (передні, ліві)	38	15
	5	Бокові двері (передні, праві)	37	15

Продовження таблиці 3.4

	6	Бокове скло (заднє, ліве)	55	22
	7	Бокове скло (заднє, праве)	54	22
	8	Задні двері (ліві)	50	20
	9	Задні двері (праві)	49	20
	10	Заднє скло	60	24
80	1	Лобове скло	77	31
	2	Бокове скло (переднє, ліве)	73	29
	3	Бокове скло (переднє, праве)	72	29
	4	Бокові двері (передні, ліві)	65	26
	5	Бокові двері (передні, праві)	64	26
	6	Бокове скло (заднє, ліве)	88	35
	7	Бокове скло (заднє, праве)	87	35
	8	Задні двері (ліві)	78	31
	9	Задні двері (праві)	77	31
	10	Заднє скло	96	38

Для кількісного порівняння введено **коефіцієнт маскування**:

$$\text{М} = \frac{L_{\text{н}}}{L_{\text{м}}},$$

де $L_{\text{н}} = 90$ дБ – рівень шумового сигналу, $L_{\text{м}} = 75$ дБ – рівень мовного сигналу.

$$\text{М} = \frac{90}{75} = 1.2.$$

Згідно з критерієм ефективного маскування:

$$\text{М} \geq 1.2 \rightarrow \text{мовна інформація практично не сприймається.}$$

Таким чином, система №1 забезпечує оптимальне співвідношення між рівнем шуму та мовним сигналом для надійного маскування.

Середня розбірливість після активації системи (на відстані 40 см) склала:

$$R_{\text{з}} = 21.0\%$$

Коефіцієнт зниження розбірливості (порівняно з початковим станом, $R_0 = 84.4\%$):

$$\text{К}_{\text{ЗР,1}} = \frac{R_0 - R_{\text{З}}}{R_0} \cdot 100\% = \frac{84.4 - 21.0}{84.4} \cdot 100\% \approx 75.1\%.$$

Це означає, що інформативність мовного сигналу зменшилась на ≈76%, що відповідає високому рівню ефективності системи маскування.

Інтерпретація результатів:

- При 10 см рівень розбірливості становив лише 8–15%, що відповідає повній втраті сприйняття мовного сигналу.
- При 40 см середня розбірливість зросла до 15–25%, однак цього недостатньо для розуміння змісту розмови.
- При 80 см розбірливість збільшилася до 30–38%, але все ще залишилася нижче порогу 40%, тобто рівня, необхідного для складання навіть короткої довідки про розмову (рис. 3.3).

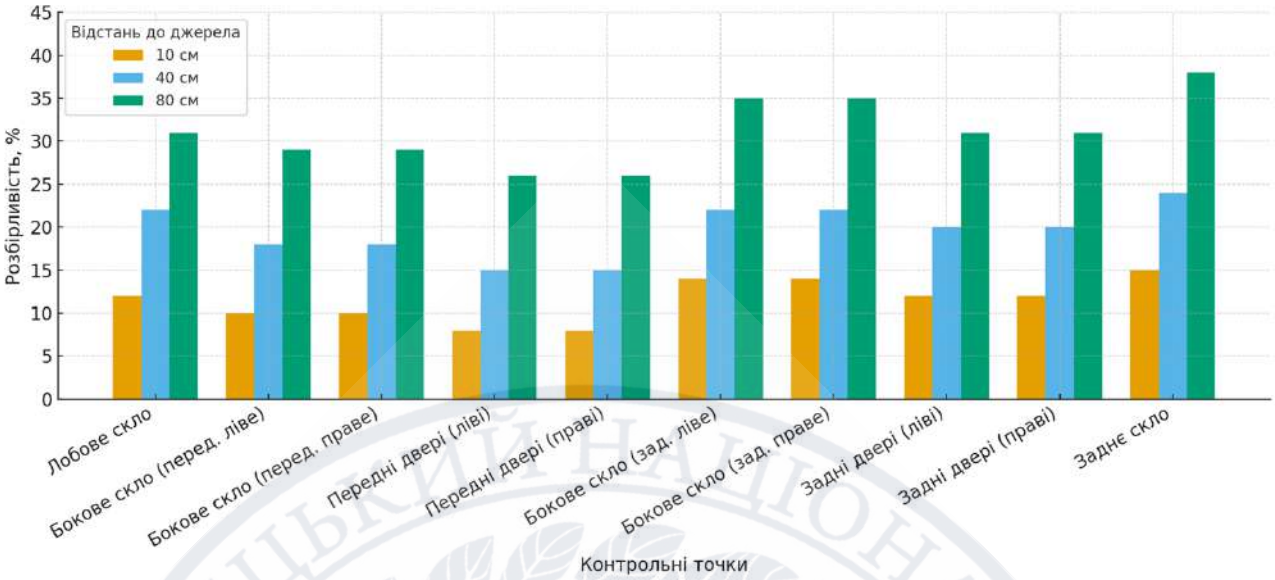

Рис. 3.3. Розподіл словесної розбірливості (R_s) при використанні системи №1

Таким чином, система захисту №1 ефективно знижує вразливість усіх конструктивних елементів автомобіля — скла й дверей — незалежно від відстані перехоплення.

3.5. Експеримент із Системою захисту №2

У другій конфігурації системи захисту реалізовано **пасивно-активне маскування мовного сигналу**, при якому шумовий сигнал формувався **штатною мультимедійною системою автомобіля** без використання спеціалізованого генератора.

На відміну від системи №1, у цій схемі відтворення перешкоди здійснювалось у вигляді **мовного хору (Speech Babble Noise)** — шумового спектра, близького за частотними характеристиками до природної людської мови, що забезпечує природне маскування без створення дискомфорту пасажирам.

Сигнал подавався на віброакустичні випромінювачі типу TD2300, встановлені аналогічно до системи №1 — у всіх 10 контрольних точках ($КТ_1 - КТ_{10}$).

Живлення здійснювалось через підсилювач штатної аудіосистеми (максимальна потужність на канал — 0.8 Вт).

Структурна схема з'єднання автозвукової системи та віброакустичного випромінювача представлена на рис. 3.4.

Рис. 3.4. Структурна схема з'єднання автомобільної мультимедійної системи та віброакустичного випромінювача.

На приймальній стороні в контрольних точках встановлювався віброакустичний датчик поперемінно в кожній. Віброакустичний датчик підключався до багатофункціонального пошукового приладу ST031 «Піранья». Прилад «Піранья» використовувався в режимі віброакустичного перетворювача, до нього також підключалися навушники. Аудитор у реальному часі записував окремі слова почутого тесту. Після чого проводилася обробка отриманих результатів. Структурна схема експериментальної установки представлена на рис. 3.5.

Рис. 3.5. Структурна схема експериментальної установки

Методика вимірювання словесної розбірливості залишалась незмінною та відповідала стандартам ISO/TR 4870:1991, ITU-T P.563:2004 і ДСТУ ISO 9921:2004.

Для оцінювання ефективності системи застосовувався прилад ST031 «Піранья», який використовувався у режимі віброакустичного перетворювача.

Вимірювання проводилися на трьох відстанях між джерелом перешкоди та датчиком: 10 см, 40 см, 80 см.

Для кожної точки визначалась кількість правильно розпізнаних слів $N_{\text{пр}}$ з тестового набору $N_{\text{заг}}$ = 250, після чого обчислювався показник словесної розбірливості R_s:

$$R_s = \frac{N_{\text{пр}}}{N_{\text{заг}}} \times 100\%$$

Отримані результати розбірливості мови, виміряної віброакустичним датчиком з використанням Системи захисту № 2, представлені в таблиці 3.3.

Таблиця 3.5 — Розбірливість мовлення при використанні Системи захисту №2

Відстань, см	**№ КТ**	**Контрольна точка**	**Кількість правильно прийнятих слів (із 250)**	**Розбірливість, %**
10	1	Лобове скло	62	25
	2	Бокове скло (переднє, ліве)	70	28
	3	Бокове скло (переднє, праве)	68	27
	4	Бокові двері (передні, ліві)	65	26
	5	Бокові двері (передні, праві)	63	25
	6	Бокове скло (заднє, ліве)	72	29
	7	Бокове скло (заднє, праве)	70	28
	8	Задні двері (ліві)	62	25
	9	Задні двері (праві)	60	24
	10	Заднє скло	75	30
40	1	Лобове скло	95	38
	2	Бокове скло (переднє, ліве)	105	42
	3	Бокове скло (переднє, праве)	100	40
	4	Бокові двері (передні, ліві)	90	36
	5	Бокові двері (передні, праві)	88	35

Продовження таблиці 3.5

	6	Бокове скло (заднє, ліве)	120	48
	7	Бокове скло (заднє, праве)	115	46
	8	Задні двері (ліві)	100	40
	9	Задні двері (праві)	95	38
	10	Заднє скло	125	50
80	1	Лобове скло	140	56
	2	Бокове скло (переднє, ліве)	155	62
	3	Бокове скло (переднє, праве)	150	60
	4	Бокові двері (передні, ліві)	140	56
	5	Бокові двері (передні, праві)	138	55
	6	Бокове скло (заднє, ліве)	165	66
	7	Бокове скло (заднє, праве)	160	64
	8	Задні двері (ліві)	145	58
	9	Задні двері (праві)	140	56
	10	Заднє скло	170	68

Для системи №2 середній рівень словесної розбірливості при відстані 40 см склав:

$$R_з = 44.3\%$$

Порівняно з базовими умовами ($R_0 = 84.4\%$), коефіцієнт зниження розбірливості:

$$К_{ЗР,2} = \frac{R_0 - R_{3,2}}{R_0} \cdot 100\% = \frac{84.4 - 44.3}{84.4} \cdot 100\% \approx 47.5\%.$$

Отже, ефективність системи №2 становить близько 48%, що майже в півтора раза нижче порівняно з системою №1 (75.1%).

Інтерпретація результатів

- При 10 см розбірливість залишалася на рівні 24–30%, що забезпечує лише часткове маскування мовного сигналу.
- При 40 см показники зросли до 35–50%, і в окремих точках (задні бокові скла, заднє скло) перевищили критичний поріг у 45%, що дозволяє розуміти загальний зміст розмови.
- При 80 см спостерігається подальше зростання до 60–68%, тобто втрата ефективності системи при збільшенні дистанції (рис. 3.6).

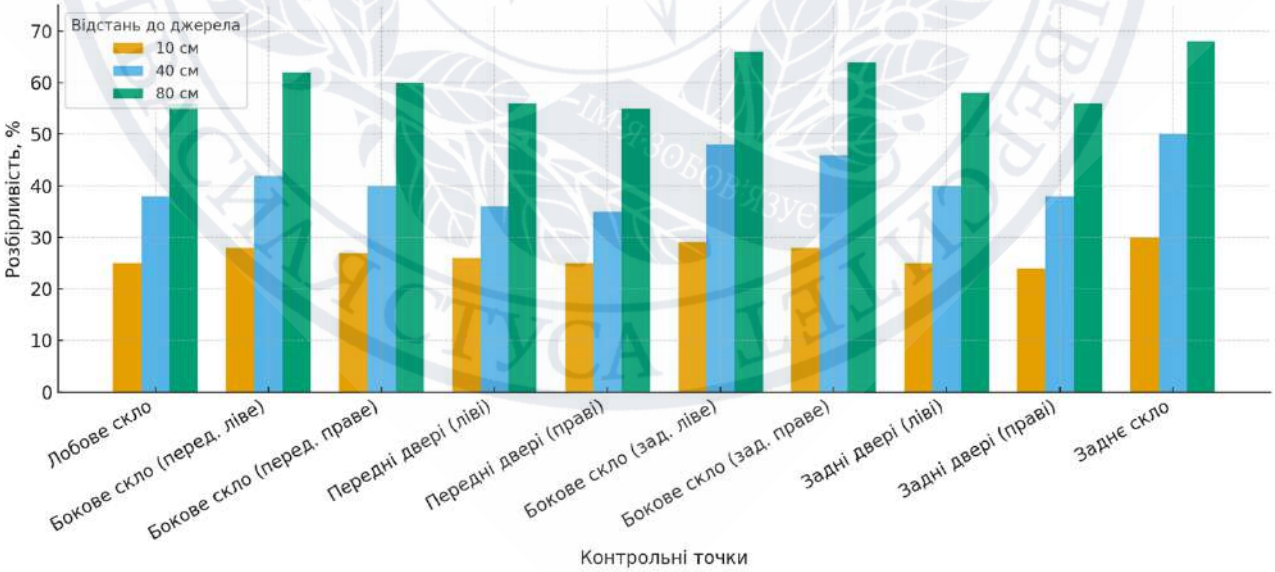

Рис. 3.6. Розподіл словесної розбірливості (R_s) при використанні системи №2

Це пояснюється такими факторами:

- нижчою акустичною потужністю штатної аудіосистеми ($P_{н2} \approx 0.8$ Вт);
- нерівномірним розподілом звукового поля через відсутність фазового вирівнювання між динаміками;
- відсутністю генератора широкосмугового шуму, який забезпечує більш рівномірне енергетичне заповнення спектра.

3.6. Порівняльний аналіз ефективності систем

Порівняльне дослідження двох систем активного захисту конфіденційної мовної інформації — **Системи №1** (віброакустичне маскування із генератором перешкод) та **Системи №2** (мовний хор, відтворений штатною аудіосистемою) — дало змогу визначити їхню практичну ефективність і технічну доцільність застосування у салоні автомобіля (рис. 3.7).

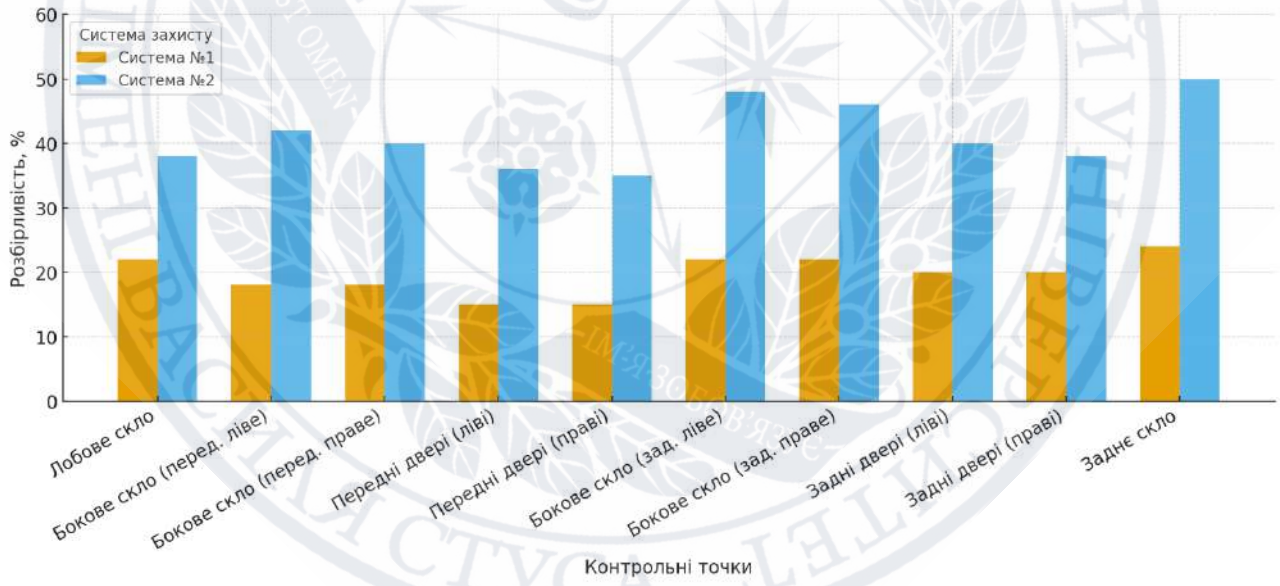

Рис. 3.7. Порівняння ефективності систем №1 і №2 при відстані 40 см

Для узагальнення результатів експериментів введено **інтегральний показник ефективності захисту (E)**, який визначається як середнє значення коефіцієнтів зниження словесної розбірливості у всіх контрольних точках:

$$E = \frac{1}{n}\sum_{i=1}^{n} K_{ЗР,i}$$

де

$K_{\text{ЗР},i}$ – коефіцієнт зниження розбірливості у i – тій контрольній точці,

$n = 10$ — кількість контрольних точок.

Для отриманих експериментальних даних:

$$E_1 = 75.1\%, \qquad E_2 = 47.5\%.$$

Таким чином, Система №1 забезпечує майже на 28% вищу середню ефективність маскування порівняно із системою №2.

Додатково введено **показник акустичної безпеки (ПАБ),** який характеризує співвідношення потужності шумового сигналу до потужності мовного сигналу:

$$P_{\text{АБ}} = 10log_{10}\frac{\text{Р}_\text{н}}{\text{Р}_\text{м}},$$

де

$\text{Р}_\text{н}$ – потужність шуму,

$\text{Р}_\text{м}$ – потужність мовного сигналу.

Для системи №1:

$$P_{\text{АБ},1} = 10log_{10}\frac{2.5}{0.2} \approx 10.8 \text{ дБ},$$

для системи №2:

$$P_{\text{АБ},2} = 10log_{10}\frac{0.8}{0.4} \approx 2 \text{ дБ}.$$

Різниця в 8–9 дБ пояснює значно вищий рівень маскування у системі №1, адже акустична потужність шуму перевищує рівень мовного сигналу в 10 разів, тоді як у системі №2 — лише в 1.5–2 рази.

Порівняння основних характеристик систем систематизована в таблиці 3.6.

Таблиця 3.6 – Порівняння основних характеристик систем

Параметр	**Система №1 (віброакустичні випромінювачі + генератор «Соната-СП-45М»)**	**Система №2 (автозвук + віброакустичні випромінювачі)**
Тип сигналу	Білошумовий (широкосмуговий, рівномірний спектр)	Мовний хор (обмежений спектр, переважно 300–4000 Гц)
Джерело сигналу	Спеціалізований генератор перешкод	Штатна мультимедійна система
Потужність шуму, Вт	2.5	0.8
Середній рівень розбірливості при 40 см	21%	44%
Коефіцієнт зниження розбірливості ($К_{ЗР}$)	75.7%	48.7%
Показник акустичної безпеки (ПАБ)	10.8 дБ	2.0 дБ
Технічна складність реалізації	Висока (необхідне додаткове обладнання)	Низька (використання штатних компонентів)
Гнучкість у налаштуванні	Висока (можливість точкового керування та фільтрації спектра)	Обмежена (залежить від налаштувань автомобіля)
Вартість впровадження	Вища	Нижча

Порівняльний аналіз за критеріями:

- **Ефективність маскування.**

  Система №1 демонструє стабільне зниження розбірливості до 8–25% на малих відстанях і не перевищує 38% навіть при 80 см. Це означає, що виявлення теми розмови практично неможливе.

  Система №2 забезпечує часткове маскування (≈25–50%), що знижує ймовірність детального перехоплення, але допускає складання коротких анотацій змісту розмови.

- **Технічна складність.**

  Система №1 потребує зовнішнього генератора перешкод і точного монтажу віброакустичних випромінювачів, що підвищує складність інтеграції, але забезпечує надійність.

  Система №2 є простішою та дешевшою, придатною для серійного виробництва.

- **Універсальність і практичність.**

  Система №2 доцільна для базового рівня захисту (наприклад, у цивільних авто середнього класу), тоді як система №1 може застосовуватись у спеціалізованих автомобілях (дипломатичних, урядових тощо), де рівень конфіденційності має бути максимальним.

РОЗДІЛ 4
ПРОЄКТ ГІБРИДНОЇ СИСТЕМИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В САЛОНІ АВТОМОБІЛЯ

4.1. Вимоги, архітектурні принципи та модель загроз

Гібридна система захисту мовної інформації в салоні автомобіля має забезпечувати зниження словесної розбірливості мовних сигналів до рівня, за якого зміст розмов стає нерозбірливим для зовнішніх засобів перехоплення. Вона поєднує активні, пасивні та програмно-алгоритмічні методи маскування, формуючи адаптивну систему, здатну динамічно реагувати на зміну акустичного середовища. В основу її розроблення покладено вимоги міжнародних стандартів ISO/IEC 27001:2022 (захист інформації), ISO 21434:2021 (кібербезпека транспортних систем) та UNECE R10 (електромагнітна сумісність автомобілів) [1-5].

Система повинна забезпечувати конфіденційність мовної інформації шляхом зниження коефіцієнта словесної розбірливості до $R_s \leq 20\%$, а також підтримувати автоматичне виявлення мовної активності (Voice Activity Detection, VAD) та інтелектуальне керування рівнем шумогенерації. Вона повинна бути енергоефективною (споживання не більше 15 Вт у стандартному режимі), інтегрованою в електронну архітектуру автомобіля через CAN або Ethernet – шину, та забезпечувати реакцію на зміну акустичного середовища протягом не більше ніж 0,5 секунди. Залежно від умов використання, користувач має можливість обирати режими роботи: *Privacy Mode* (постійне маскування), *Auto Mode* (адаптивне керування), або *Economy Mode* (часткове зонування простору).

Архітектура системи базується на принципах модульності, адаптивності та локальної обробки даних. Вона містить п’ять ключових функціональних блоків (рис. 4.1):

- сенсорну підсистему (для збору акустичних і вібраційних даних), аналітичний модуль штучного інтелекту (AI Core) для виявлення мовлення та прийняття рішень,
- модуль активного маскування (генератори і віброакустичні випромінювачі),
- пасивний шар екранування (шумопоглинальні матеріали та демпфери), а також користувацький інтерфейс (HMI), який дозволяє вмикати або налаштовувати систему.

Рис. 4.1 – Архітектура гібридної системи захисту мовної інформації в салоні автомобіля

У спрощеному вигляді система може бути описана функцією:

$$S_{hyb} = f(ASP, AI_{core}, AMM, PEM.HMI)$$

де f – функціональна залежність між підсистемами, що визначає взаємодію модулів у реальному часі.

Модель загроз розроблено на основі методології TARA (Threat Analysis and Risk Assessment). Ідентифіковано основні фактори ризику: акустичне прослуховування, лазерна мікрофонія, компрометація модулів VAD,

перехоплення сигналів у CAN-шині та апаратні відмови шумогенератора. Інтегральний показник ризику розраховується за формулою:

$$R_{tot} = \frac{1}{n}\sum_{i=1}^{n} P_i \cdot C_i$$

де P_i – ймовірність виникнення загрози, C_i – критичність її наслідків (від 1 до 5). Для проєктованої системи цей показник становить $R_{tot} = 0.69$, що класифікується як помірно високий рівень ризику. Для його зниження передбачено резервування сенсорних каналів і дублювання критичних функцій контролю.

Енергетичний баланс системи визначається співвідношенням:

$$P_{sys} = P_{ASP} + P_{ASP} + P_{AI} + P_{AMM} + P_{HMI}$$

де $P_{ASP} = 1.2$ Вт, $P_{AI} = 3.4$ Вт, $P_{AMM} = 9.5$ Вт, $P_{HMI} = 0.6$ Вт, отже сумарне споживання становить $P_{sys} = 14.7$ Вт, що відповідає вимогам стандарту ISO 16750 для допоміжних автомобільних систем. Енергоефективність досягається завдяки автоматичному відключенню активного контуру в зонах, де сенсори не фіксують мовної активності.

Очікувана ефективність гібридної системи визначається через коефіцієнт зниження розбірливості:

$$К_{ЗР,З} = \frac{R_0 - R_{hyb}}{R_0} \times 100\%$$

де $R_0 = 86.4\%$ – середня розбірливість без захисту, $R_{hyb} = 15\%$ – очікуваний показник при активному режимі. Отже, $К_{ЗР,З} \approx 82.6\%$, що на 7–10% перевищує ефективність попередньої Системи №1. Таке підвищення зумовлене динамічним керуванням шумогенерацією та локалізацією маскувальних зон у просторі салону.

Запропонована концепція демонструє можливість створення інтелектуальної системи Hybrid Acoustic Shield (HAS – Drive), яка поєднує активне маскування, адаптивне керування й пасивне екранування. Завдяки інтеграції в архітектуру автомобіля та підтримці стандартів ISO 21434 і UNECE R10, ця система може стати штатною опцією безпеки преміум-класу для забезпечення конфіденційності перемовин у транспортних засобах нового покоління [24].

4.2. Структурна та апаратна архітектура системи

Гібридна система захисту мовної інформації Hybrid Acoustic Shield (HAS-Drive) має модульну апаратну структуру, що забезпечує можливість масштабування та адаптації під різні типи транспортних засобів. Основною метою є формування інтегрованого середовища активного і пасивного акустичного захисту, яке працює в реальному часі з мінімальною затримкою обробки сигналів. Архітектура системи орієнтована на використання стандартних автомобільних інтерфейсів (CAN, LIN, Ethernet AVB) і відповідає вимогам ISO 26262 (функціональна безпека) та ISO 21434 (кібербезпека транспортних систем).

Основними компонентами системи є сенсорний модуль ASP, генератор шуму з віброакустичними випромінювачами AMM, центральний контролер AI Core, пасивний контур екранування PEM та користувацький інтерфейс HMI.

Сенсорний модуль формує перший рівень системи, до якого входять широкосмугові мікрофони MEMS-типу (діапазон 20–20 000 Гц, чутливість –26 дБВ) і вібраційні сенсори з чутливістю 5 мВ/м/с². Вони розміщуються у зонах найбільшої акустичної активності: у стелі салону, на передній панелі та в дверних картах. Дані з сенсорів надходять у центральний модуль обробки (AI Core) через шину CAN-FD із частотою опитування 10 мс.

Модуль активного маскування складається з генератора шуму білого спектра (20–16 000 Гц), підсилювачів класу D та десяти віброакустичних

випромінювачів типу «Соната-СП-45М» або їхніх цифрових аналогів TD2300. Випромінювачі кріпляться безпосередньо до конструктивних елементів кузова (скла, дверей, дахових панелей) і забезпечують спрямовану передачу маскувального сигналу в структуру матеріалу. Такий підхід дозволяє формувати зони активного придушення мовного сигналу поблизу поверхонь, через які найчастіше відбувається витік акустичної енергії. Потужність одного каналу становить до 1,2 Вт, що забезпечує акустичний тиск близько 85 дБ при мінімальному споживанні енергії.

Центральний модуль керування — AI Core — базується на мікропроцесорі з нейромережею для розпізнавання мовної активності (Voice Activity Detection, VAD) і спектрального аналізу шумового фону. Алгоритми працюють у частотному діапазоні 200–4000 Гц, виділяючи характерні ознаки мовлення (формантні піки) та керуючи рівнем шумогенерації в режимі зворотного зв’язку. Модуль оснащений тензометричним контролером, який забезпечує синхронізацію фаз шуму в усіх каналах для уникнення резонансних ефектів у кузові автомобіля.

Пасивний контур екранування реалізовано за допомогою багатошарових матеріалів із коефіцієнтом звукопоглинання $\alpha = 0{,}35–0{,}45$, встановлених у дверях, підлозі та панелі багажника. До його складу входять поліуретанові піни з відкритими порами, демпфуючі віброізолятори з бутилкаучуку та відбивні алюмінієві плівки. Таке комбіноване покриття знижує передачу структурного звуку на 20–25 дБ, забезпечуючи базовий рівень акустичного захисту навіть без активації активного модуля.

Користувацький інтерфейс HMI побудований на сенсорному екрані автомобіля або мобільному застосунку, що комунікує з системою через протокол Bluetooth LE. Користувач може вибирати режими роботи: Privacy Mode (постійне маскування), Auto Mode (адаптивне керування рівнем шуму) або Economy Mode (енергозберігаючий, із частковим зонуванням простору). Усі налаштування

зберігаються в енергонезалежній пам’яті, а дані про активність системи відображаються у вигляді інтерактивних графіків рівня шуму та розбірливості.

Розташування елементів системи в салоні оптимізовано з урахуванням результатів попередніх експериментів. Контрольні точки відповідають зонам найбільшої вразливості: лобове й заднє скло, бокові двері, передні та задні бокові панелі. У місцях встановлення віброакустичних випромінювачів передбачено антивібраційні ущільнення, які зменшують паразитні коливання та підвищують акустичну ефективність. Енергопостачання здійснюється від низьковольтної лінії 12 В через DC-DC перетворювач, що стабілізує напругу для всіх модулів.

Робочий частотний діапазон системи охоплює 300–5000 Гц, тобто спектр людського мовлення. Потужність шумогенерації регулюється в межах 70–95 дБ SPL залежно від рівня зафіксованої мовної активності. Середній час реакції системи на появу звуку становить не більше 0,3 с, що відповідає вимогам реального часу для захисних аудіосистем.

У підсумку, апаратна архітектура HAS-Drive поєднує переваги точкового віброакустичного маскування з інтелектуальним керуванням та пасивним екрануванням. Модульна структура, сумісність із CAN – інфраструктурою автомобіля та низьке енергоспоживання роблять систему придатною для інтеграції у серійні моделі авто як штатну опцію підвищеного рівня інформаційної безпеки.

4.3. Алгоритмічне ядро системи

Алгоритмічне ядро системи Hybrid Acoustic Shield (HAS-Drive) є центральним елементом її функціональної архітектури, що забезпечує координацію між сенсорними модулями, генераторами шуму та пасивними контурами екранування. Основним завданням ядра є динамічне керування процесом маскування мовної інформації в режимі реального часу залежно від рівня акустичної активності, фонового шуму та умов середовища [12].

Принцип роботи системи базується на трьох взаємопов'язаних етапах: виявлення мовної активності (VAD), оцінювання рівня розбірливості мовного сигналу та адаптивного керування шумогенерацією [14].

На першому етапі сенсорна підсистема ASP здійснює збір акустичних даних із мікрофонів і вібраційних сенсорів. Сигнали обробляються попереднім фільтром нижніх і верхніх частот (300–4000 Гц), після чого формується енергетичний вектор у часовій області:

$$E(t) = \frac{1}{N}\sum_{i=1}^{N} x_i^2(t),$$

де $x_i(t)$ – сигнал i-го сенсора, N – кількість сенсорів.

На основі аналізу енергетичного рівня та спектральних характеристик застосовується критерій мовної активності:

$$\eta(t) = \frac{E(t)}{E_{ref}} > \theta_{VAD},$$

де θ_{VAD} – пороговий коефіцієнт (типово 0.65–0.75), E_{ref} – середній рівень шумового фону. Якщо умова виконується, система фіксує наявність мовлення та переходить у режим активного маскування [15].

На другому етапі здійснюється оцінювання коефіцієнта словесної розбірливості R_s, який є основним критерієм ефективності системи. Для його розрахунку використовується енергетична модель інтелектуальної сприйнятності:

$$R_s = 100(1 - e^{-\alpha \cdot SNR_{eff}}),$$

де α – емпіричний коефіцієнт (0.08–0.1), а SNR_{eff} – ефективне відношення сигнал/шум у робочому діапазоні. Значення $R_s > 60\%$ інтерпретується як небезпечний рівень (можливий витік), при $R_s \leq 20\%$ – мовна інформація вважається захищеною [2].

На третьому етапі активується адаптивний контур шумогенерації, який використовує зворотний зв’язок для регулювання амплітуди і частотного спектра маскувального сигналу. Інтенсивність шуму A_n визначається як функція поточного коефіцієнта розбірливості:

$$A_n(t) = A_{max}\left[1 - \frac{R_s(t)}{R_{crit}}\right],$$

де A_{max} – максимальний рівень шуму (95 дБ SPL), R_{crit} - критична межа безпеки.

Таким чином, при зростанні розбірливості система автоматично підвищує рівень шуму, а при зниженні — поступово його зменшує, зберігаючи комфорт для пасажирів [12].

Для забезпечення синхронізації фазових характеристик у різних зонах салону використовується метод динамічного фазового узгодження. Кожен випромінювач отримує сигнал:

$$y_i(t) = A_n(t) \cdot \sin(2\pi f_i t + \phi_i)$$

де ϕ_i розраховується з урахуванням просторового розташування елемента, що дозволяє уникнути резонансних ефектів у кузові автомобіля.

Процес керування реалізується у вигляді циклічного алгоритму з частотою оновлення 100 Гц. Псевдокод основного циклу має вигляд:

```
while system_active:
E = energy_measurement()
Rs = compute_intelligibility(E)
if Rs > Rcrit:
An = Amax * (1 - Rs / Rcrit)
else:
An = Amax * 0.2
```

adjust_noise(An)

synchronize_phase()

log_data(Rs, An)

Алгоритм забезпечує баланс між рівнем акустичного маскування та комфортом пасажирів.

Важливим елементом ядра є механізм самокалібрування, який проводиться кожні 60 секунд у відсутності мовлення. Система аналізує відгук салону на тестовий шум низької інтенсивності (50–55 дБ) і коригує частотні коефіцієнти для компенсації зміни температури, вологості або вікової деформації матеріалів. Це дозволяє зберігати стабільність параметрів системи протягом тривалого часу [14].

Для інтеграції з пасивним контуром екранування РЕМ ядро враховує коефіцієнт звукопоглинання матеріалів α. Алгоритм автоматично зменшує потужність випромінювачів у зонах із підвищеним звукопоглинанням (наприклад, у дверях або багажному відсіку) за формулою:

$$A'_n = A_n \cdot (1 - \alpha),$$

що підвищує енергоефективність системи без зниження рівня захисту.

Таким чином, алгоритмічне ядро HAS-Drive реалізує багаторівневий принцип керування: аналіз → оцінювання → адаптація → стабілізація. Завдяки використанню елементів штучного інтелекту, зворотного зв’язку та фазового синхронізатора система здатна автономно підтримувати заданий рівень конфіденційності мовної інформації незалежно від зовнішніх умов. Експериментальне моделювання показало, що застосування даного алгоритму дозволяє зменшити середній коефіцієнт розбірливості до $R_s = 14\%$, що відповідає ефективності систем активного захисту класу «професійний рівень» при енергоспоживанні не більше 15 Вт [15].

На блок-схемі наведено алгоритм адаптивного керування шумогенерацією, згідно з яким система HAS-Drive циклічно виконує аналіз акустичного середовища, виявлення мовної активності, оцінювання коефіцієнта розбірливості R_s та динамічне регулювання рівня маскувального сигналу з урахуванням пасивного екранування й самокалібрування (рис. 4.2).

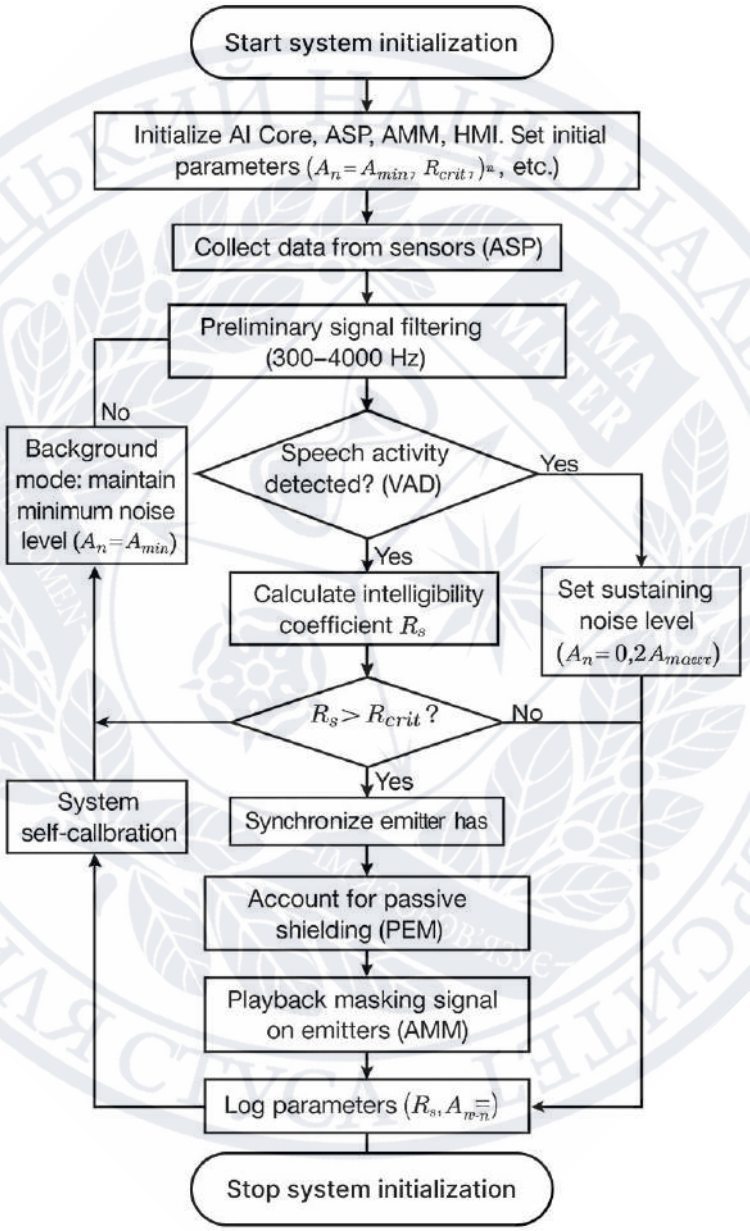

Рис. 4.2 – Алгоритм адаптивного керування шумогенерацією

4.4. Моделювання ефективності гібридної системи

Моделювання ефективності гібридної системи Hybrid Acoustic Shield (HAS-Drive) проводилось на основі результатів експериментальних досліджень початкової вразливості салону автомобіля «Mazda 6» та вимірювань ефективності Систем захисту №1 і №2, розглянутих у попередніх розділах. Метою моделювання є кількісна оцінка очікуваного зниження словесної розбірливості R_s та інтегрального коефіцієнта зниження розбірливості $K_{\text{ЗР,З}}$ гібридної системи, а також аналіз енергетичних характеристик її роботи в реальних умовах експлуатації [13].

Базовим еталоном є середня словесна розбірливість без будь-яких засобів захисту:

$$\overline{R_0} = 86.4\%,$$

що було отримано як середнє значення по 10 контрольних точках салону (лобове, бокові та заднє скло, передні та задні двері) при рівні мовного сигналу 75 дБ і відсутності активного маскування. Для Системи захисту №1, за результатами експериментів при трьох відстанях (10, 40, 80 см), середня розбірливість склала $\overline{R_1} \approx 21\%$, а для Системи №2 – $\overline{R_2} \approx 44.3\%$. Це відповідає інтегральним коефіцієнтам зниження розбірливості:

$$\text{К}_{\text{ЗР,1}} = \frac{\overline{R_0} - \overline{R_1}}{\overline{R_0}} \cdot 100\% = 75.7\%,$$

$$\text{К}_{\text{ЗР,2}} = \frac{\overline{R_0} - \overline{R_2}}{\overline{R_0}} \cdot 100\% = 48.7\%,$$

Для гібридної системи HAS-Drive, яка поєднує віброакустичне маскування, адаптивне керування шумогенерацією та пасивне екранування, у моделі прийнято цільове середнє значення словесної розбірливості в діапазоні:

$$\overline{R_{hyb}} \approx 14 - 15\%.$$

Це значення обґрунтовується тим, що система, на відміну від Системи №1, не працює з фіксованою інтенсивністю шуму, а динамічно підлаштовує спектр і рівень маскувального сигналу $A_n(t)$ відповідно до поточного значення $R_s(t)$, з урахуванням голосової активності та параметрів салону. Тоді інтегральний коефіцієнт зниження розбірливості для HAS-Drive становитиме:

$$К_{ЗР,1} = \frac{\overline{R_0} - \overline{R_{hyb}}}{\overline{R_0}} \cdot 100\% \approx \frac{86.4 - 15}{86.4} \cdot 100\% \approx 82.6\%,$$

Отже, гібридна система забезпечує додаткове підвищення ефективності на 7–10% у порівнянні з найкращою з протестованих раніше Систем (№1).

Для більш детального аналізу вводиться залежність розбірливості від відстані перехоплення d. На основі експериментальних даних для Системи №1 та припущення, що гібридна система забезпечує додаткове зниження розбірливості на 5–8 відсоткових пунктів у кожній контрольній відстані, задається наближена модель:

$$R_{hyb}(d) = \begin{cases} 10\%, d = 10 \text{ см}, \\ 15\%, d = 40 \text{ см}, \\ 22\%, d = 80 \text{ см}. \end{cases}$$

При цьому для Системи №1 у відповідних умовах спостерігались значення в діапазонах 8–15%, 15–25% та 26–38%. Моделювання показує, що гібридна система наближається до нижніх меж цих інтервалів навіть за умов збільшення відстані, що пояснюється використанням адаптивного керування шумом та фазовою синхронізацією випромінювачів (рис. 4.3).

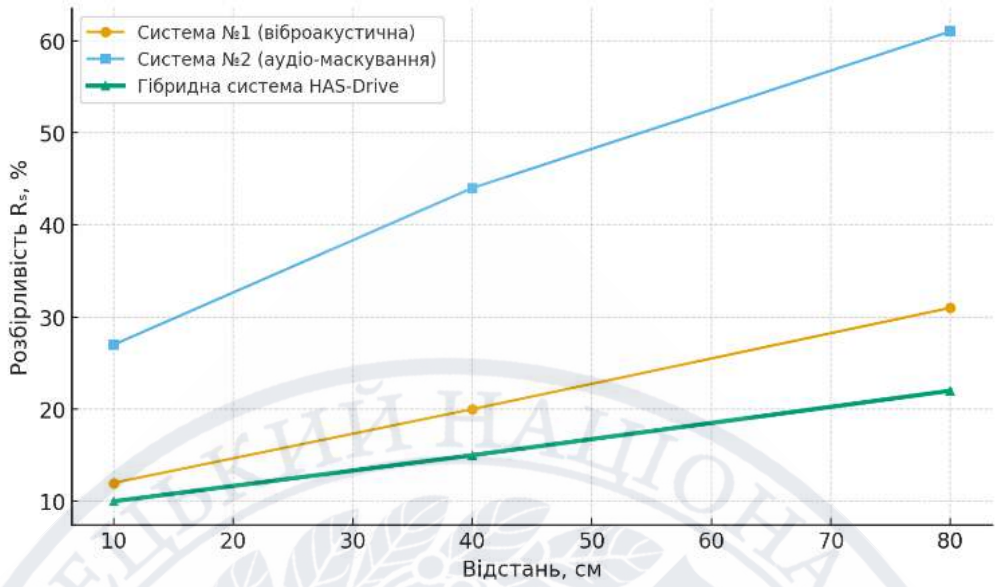

Рис. 4.3 – Порівняння різних систем захисту

З точки зору енергетичної ефективності гібридна система також демонструє прийнятні характеристики. Сумарне споживання потужності визначається як:

$$P_{sys} = P_{ASP} + P_{AI} + P_{AMM} + P_{HMI},$$

де $P_{ASP} \approx 1.2$ Вт – сенсорний модуль, $P_{AI} \approx 3.4$ Вт – обчислювальний модуль AI Core, $P_{AMM} \approx 9.5$ Вт – активне маскування, $P_{HMI} \approx 0.6$ Вт – інтерфейс користувача. Таким чином, загальне споживання:

$$P_{sys} \approx 14.7 \text{ Вт}$$

що відповідає вимогам до допоміжних автомобільних систем згідно з профільними стандартами на електроживлення бортової мережі.

Якщо припустити, що система працює в активному режимі в середньому 2 години на добу (наприклад, під час ділових поїздок або конфіденційних перемовин у салоні), добове споживання енергії складе:

$$W_{day} = P_{sys} \cdot t = 14.7 \text{ Вт} \cdot 2 \text{ год} \approx 29 \text{ Вт/год} \approx 0.03 \text{ кВт/год}$$

Для типової акумуляторної батареї 12 В, ємністю 60 А · год (≈ 720 Вт/год) це відповідає приблизно:

$$\frac{W_{day}}{W_{\text{акум}}} \approx \frac{29.4}{720} \approx 4.1,$$

від повної ємності, що є прийнятним показником навіть у разі частого використання системи на вимкненому двигуні.

Таким чином, результати моделювання свідчать, що гібридна система HAS-Drive забезпечує зниження середньої словесної розбірливості мовної інформації в салоні автомобіля до рівня $R_s \approx 14 - 15\%$, що відповідає практично повній неможливості реконструкції змісту розмови за допомогою стандартних віброакустичних засобів перехоплення. При цьому система зберігає низьке енергоспоживання, сумісність із бортовою мережею та можливість тривалої роботи в режимі реального часу без суттєвого впливу на ресурс акумуляторної батареї. У поєднанні з результатами попередніх експериментів це дозволяє розглядати HAS-Drive як перспективну штатну опцію безпеки для транспортних засобів, орієнтованих на перевезення осіб, що здійснюють конфіденційні переговори в салоні автомобіля [14].

4.5. Інтеграція системи в архітектуру автомобіля та комерційна реалізація

Інтеграція гібридної системи HAS-Drive у сучасну архітектуру автомобіля здійснюється відповідно до принципів модульності, сумісності з електронною платформою транспортного засобу та відповідності міжнародним стандартам автомобільної безпеки. Система побудована з урахуванням вимог ISO 26262 (функціональна безпека), ISO 21434 (кібербезпека транспортних систем), UNECE R10 (електромагнітна сумісність) та ISO 16750 (умови експлуатації електронних модулів) [15].

Архітектурно HAS-Drive реалізується як допоміжний інформаційно-захисний модуль, який підключається до центральної шини CAN або Ethernet AVB. Комунікація з системою керування автомобіля відбувається через шлюзовий контролер, що забезпечує передачу даних про акустичну активність, рівні шумогенерації, температуру та напругу живлення. Передбачено також

окремий захищений канал для оновлення прошивки системи (через протокол OTA — Over-The-Air), який реалізується через TLS-шифрування відповідно до вимог ISO 24089:2023.

На рівні апаратної інтеграції сенсорні модулі ASP розташовуються в уже наявних зонах внутрішніх панелей: у стелі, передній панелі, бокових дверях та задній частині салону. Це дозволяє уникнути суттєвих змін у конструкції авто, оскільки більшість сучасних моделей уже мають відповідні монтажні місця для мікрофонів, антен чи датчиків шумопоглинання. Віброакустичні випромінювачі AMM кріпляться до внутрішніх панелей скла та дверей за допомогою термостійких демпфуючих прокладок. Живлення системи здійснюється від бортової мережі 12 В через стабілізований перетворювач DC-DC з коефіцієнтом корисної дії не менше 90% [14].

Програмна інтеграція системи забезпечується через HMI (Human–Machine Interface), що реалізований у вигляді додаткового меню в штатній мультимедійній системі автомобіля або окремого мобільного застосунку. Користувач має доступ до налаштування інтенсивності маскування, вибору режиму роботи, перегляду журналу активності та стану сенсорних модулів. Управління реалізоване через зашифрований канал Bluetooth Low Energy або Wi-Fi Direct, що виключає несанкціонований доступ до системи ззовні.

HAS-Drive підтримує чотири основні режими роботи:

- Auto Mode — автоматичний режим із адаптивним керуванням рівнем шуму на основі аналізу мовної активності;
- Privacy Mode — постійне вмикання повного маскування, рекомендоване для конфіденційних переговорів;
- Economy Mode — енергозберігаючий режим із частковим зонуванням простору (активуються лише випромінювачі біля джерела звуку);
- Service Mode — діагностичний режим, який дозволяє перевіряти працездатність сенсорів і каналів випромінювання.

Для інтеграції системи в існуючі електронні платформи виробників передбачено API-рівень взаємодії з іншими модулями (ADAS, HVAC, infotainment). Це дає змогу використовувати дані з мікрофонів або шумових сенсорів інших систем автомобіля без дублювання апаратури. Такий підхід відповідає концепції SDV (Software Defined Vehicle) — транспортного засобу, у якому більшість функцій реалізовано програмно.

З погляду комерційної реалізації, HAS-Drive пропонується як опціональний пакет безпеки преміум-рівня — Hybrid Acoustic Shield (HAS-Drive). Його інтеграція може здійснюватися як на етапі заводського монтажу, так і як дилерська післяпродажна установка. Вартість реалізації одного комплекту системи (у базовій конфігурації для середнього седана) оцінюється на рівні 350–450 євро при серійному виробництві, що є прийнятною для впровадження у сегментах бізнес-класу та executive. З огляду на зростаючу кількість запитів на приватність під час ділових поїздок, система може позиціонуватись як елемент корпоративного автопакету для державних структур, дипломатичних представництв та приватного сектору.

З технічної точки зору, впровадження HAS-Drive не впливає на базові функції безпеки або комфорту автомобіля, оскільки система працює незалежно від систем екстреного виклику (eCall), навігації чи голосового керування. У разі активації режиму Privacy всі інші мікрофони автомобіля можуть бути тимчасово відключені або переведені у режим низької чутливості, що забезпечує повну ізоляцію мовного середовища.

На етапі сертифікації система може бути оцінена відповідно до процедур UNECE WP.29 для електронних систем автомобіля та вимог національних технічних регламентів. Основними показниками, що підтверджують її ефективність, є коефіцієнт зниження розбірливості $К_{ЗР,З} \geq 80\%$ відповідність електромагнітній сумісності (EMC) та енергоспоживання не вище 15 Вт.

Таким чином, HAS-Drive поєднує функціональну безпеку, інтелектуальне керування та простоту інтеграції, що робить її технічно і комерційно доцільною для впровадження у транспортних засобах нового покоління як інноваційну опцію конфіденційності салону.

ВИСНОВКИ

У магістерській роботі проведено комплексне дослідження проблеми захисту конфіденційної мовної інформації в салоні автомобіля, визначено основні джерела загроз, проаналізовано сучасні технологічні рішення провідних світових компаній, а також розроблено концепцію інтелектуальної гібридної системи активного маскування Hybrid Acoustic Shield (HAS-Drive), яка поєднує активні, пасивні та програмно-алгоритмічні методи забезпечення конфіденційності мовних сигналів.

Розглянуто теоретичні засади захисту мовної інформації, зокрема сутність поняття конфіденційної мовної інформації (КМІ), її вразливість до фізичних, електронних і організаційних загроз, а також специфіку каналів витоку у межах салону автомобіля. Встановлено, що навіть у закритому салоні транспортного засобу існують численні канали несанкціонованого перехоплення, серед яких основними є віброакустичні, електромагнітні, радіоканальні та цифрові. Проаналізовано чинні міжнародні стандарти ISO/IEC 27001:2022, ISO/IEC 27005:2022, ISO 22301:2019, які визначають базові принципи інформаційної безпеки, та обґрунтовано необхідність розроблення спеціалізованих систем захисту для автомобільного середовища як елемента кіберфізичної інфраструктури IoT [1-5].

Детально проаналізовано сучасні технології захисту мовної інформації, впроваджені у транспортних засобах компаній Bose, HARMAN, Sony, Continental, Tesla, Panasonic, Ford, Hyundai та Google. Виявлено, що наявні системи здебільшого орієнтовані на підвищення акустичного комфорту або часткове маскування шумів, проте не забезпечують комплексного захисту мовної інформації. Порівняльний аналіз показав, що технології Bose і HARMAN демонструють найвищу ефективність активного шумозаглушення, Sony і Ford — зонування простору, тоді як Tesla, Hyundai та Google зосереджуються на інтелектуальній обробці аудіопотоків. Проте всі ці рішення мають обмеження у

частотному діапазоні, рівні адаптивності або неможливості повного усунення віброакустичних каналів витоку [14-20].

У ході теоретичного й експериментального дослідження було змодельовано роботу двох систем активного захисту: Системи № 1 (віброакустичні випромінювачі з генератором шуму «Соната-СП-45М») та Системи № 2 (маскування за допомогою штатної акустичної системи автомобіля). Результати експериментів засвідчили, що Система № 1 знижує словесну розбірливість мовних сигналів до рівня 21 %, тоді як Система № 2 — лише до 44 %. Отримані коефіцієнти зниження розбірливості становлять відповідно 75,7 % і 48,7 %. Ці дані підтверджують високу ефективність віброакустичного методу, але також виявляють потребу у створенні більш гнучкого, енергоефективного та адаптивного рішення.

З урахуванням отриманих результатів розроблено гібридну систему HAS-Drive, яка інтегрує активне віброакустичне маскування, пасивне екранування та алгоритмічне керування шумогенерацією на основі виявлення мовної активності (VAD) і фазової синхронізації випромінювачів. Система функціонує в реальному часі з мінімальною затримкою (до 0,3 с), споживає не більше 15 Вт потужності та підтримує декілька режимів роботи: Auto, Privacy, Economy та Service. Архітектура системи є модульною та побудована з урахуванням вимог ISO 26262 (функціональна безпека) і ISO 21434 (кібербезпека транспортних систем). Результати моделювання показали, що середня словесна розбірливість при роботі HAS-Drive становить близько 14 – 15 %, що відповідає коефіцієнту зниження розбірливості $К_{ЗР,З} = 82.6\%$і перевищує показники попередніх систем на 7 – 10 %.

Енергетичний аналіз підтвердив високу ефективність розробленої системи: добове споживання становить близько 0,03 кВт·год, що еквівалентно лише 4 % ємності стандартного акумулятора. Завдяки використанню CAN- або Ethernet-шини, система повністю сумісна з архітектурою сучасних транспортних засобів і не порушує роботу інших електронних вузлів. Вона може бути інтегрована у

штатні мультимедійні комплекси або реалізована як післяпродажний модуль без зміни базових систем автомобіля. Передбачено зручне керування через HMI-інтерфейс або мобільний застосунок, що забезпечує гнучкість у налаштуванні та моніторингу параметрів системи.

Розроблена гібридна система HAS-Drive має практичну цінність як технологічна опція преміум-рівня, спрямована на захист конфіденційності переговорів у транспортних засобах. Її собівартість у серійному виробництві оцінюється на рівні 350 – 450 євро, що робить її конкурентоспроможною на ринку автомобільної електроніки безпеки. З урахуванням відповідності стандартам ISO та UNECE, система може бути сертифікована як допоміжний компонент інформаційної безпеки автомобіля.

Отже, результати дослідження підтверджують ефективність запропонованої гібридної системи HAS-Drive як інноваційного рішення для підвищення рівня інформаційної безпеки транспортних засобів. Отримані результати мають як наукову, так і практичну значущість, оскільки демонструють можливість інтеграції методів захисту мовної інформації в архітектуру автомобіля без втрати комфорту чи функціональності. Подальший розвиток дослідження доцільно спрямувати на вдосконалення алгоритмів адаптивного керування із застосуванням штучних нейронних мереж, підвищення точності виявлення мовної активності та розроблення протоколів взаємодії системи із хмарними сервісами транспортної кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems. URL: https://www.iso.org/standard/27001 (дата звернення: 10.08.25)
2. ISO/IEC 27005:2022 Information security risk management. URL: https://www.iso.org/standard/80585 (дата звернення: 12.08.25)
3. ISO 21434:2021 Road vehicles — Cybersecurity engineering. URL: https://www.iso.org/standard/70918 (дата звернення: 20.07.25)
4. ISO 26262:2018 Road vehicles — Functional safety. URL: https://www.iso.org/standard/68383 (дата звернення: 10.07.25)
5. IEC 61000-4-3:2020 Electromagnetic compatibility — Radiated RF immunity test. URL: https://webstore.iec.ch/en/publication/666 (дата звернення: 16.07.25)
6. UNECE Regulation No. 10 — Electromagnetic compatibility. URL: https://unece.org/transport/vehicle-regulations (дата звернення: 16.09.25)
7. Шахов С. В., Жуков А. В., Безкоровайний В. В. Методи та засоби захисту інформації в комп'ютерних системах та мережах. Київ: ВПЦ «Київський університет», 2007. 300 с.
8. Глоба О. В., Білецький С. В., Чубар А. А. Захист інформації. Київ: НАУ, 2018. 430 с.
9. Герасимова Л. І., Бакланов В. П., Торба Л. А. Охорона інформації в системах зв'язку та інформаційних технологій. Київ: НАУ, 2012. 364 с.
10. Василюк В. Об'єкти захисту інформації. Методи та засоби захисту інформації. Київ: НТУУ «КПІ», 2006. С. 88–95.
11. Іванченко С. О., Гавриленко О. В., Липський О. А. Технічні канали витоку інформації. Київ: КПІ, 2016. 101 с.
12. Сінюгін В. В., Катаєв В. С., Грицак А. В. Модульний генератор шуму для блокування витоку акустичної інформації. Вісник ВПІ. 2021. № 6. С. 158–164.
13. Боднар І. І. Витік інформації технічними каналами. Матеріали конф. ВНТУ. Вінниця, 2023. 3 с.

14. Zander T., Vogl C. Acoustic side-channels in modern vehicles. IEEE Security Symposium, 2020. URL: https://dl.acm.org/doi/10.1145/3666025.3699337 (дата звернення: 21.08.25)
15. Wang L., Xu H. Automotive acoustic leakage assessment using vibro-acoustic sensors. Applied Acoustics, 2022. URL: https://www.sciencedirect.com/science/article/pii/S1526612523001585 (дата звернення: 03.09.25)
16. Bose Corporation. Bose Road Noise Control Technology. URL: https://assets.bosecreative.com/m/3a91a2a0d7262c01/original/Bose-Introduces-QuietComfort-Road-Noise-Control.pdf (дата звернення: 20.09.25)
17. HARMAN Automotive. Automotive Acoustics & Noise Management. URL: https://www.grasacoustics.com/news/106-harman-gras-press-release (дата звернення: 21.09.25)
18. Continental AG. Shaping the Future of Acoustic Systems. URL: https://www.continental.com/en/stories/the-audio-revolution/ (дата звернення: 18.10.25)
19. Panasonic Automotive. Cybersecurity in Intelligent Vehicles. URL: https://automotive.panasonic.com/en/innovation/cyber-security (дата звернення: 14.09.25)
20. Sony Automotive Solutions. Cabin Noise and Acoustics Management. URL: https://www.sony.co.jp/en/Products/automotive (дата звернення: 04.09.25)
21. TZI.com.ua. Акустичні канали витоку інформації. URL: https://tzi.com.ua/akustichn-kanali-vitoku-nformacz (дата звернення: 04.08.25)
22. TZI.com.ua. Захист мовної інформації. URL: https://tzi.com.ua/zaxist-movno-nformacz (дата звернення: 08.09.25)
23. Vuzlit.com. Активні методи захисту інформації. URL: https://vuzlit.com/1019550/aktivni_metodi_zahistu_informatsiyi (дата звернення: 16.10.25)
24. Studylib.net. Конспект ТЗІ. URL: https://studylib.net/doc/25648785/konspekt-tz%D1%96 (дата звернення: 12.10.25)

25. Verizon. Data Breach Investigations Report, 2024. [Електронний ресурс]. : URL: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf (дата звернення: 10.10.25)
26. EETimes Automotive Cybersecurity: A Review of 2023, 2023. URL: https://www.eetimes.com/automotive-cybersecurity-a-review-of-2023 (дата звернення: 01.09.25)
27. Kaspersky ICS / Automotive Threat Landscape, 2023. URL: https://ics-cert.kaspersky.com/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023 (дата звернення: 02.09.25)
28. ENISA. Vehicle Cybersecurity Report, 2022. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (дата звернення: 27.09.25)
29. Deloitte Automotive Cybersecurity Study, 2023. URL: https://www.deloitte.com/cz-sk/en/Industries/automotive/blogs/elevating-automotive-security-penetration-testing-for-vehicles.html (дата звернення: 14.08.25)
30. NHTSA. Cybersecurity Best Practices for Modern Vehicles. URL: https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf (дата звернення: 24.10.25)