

УДК 62-75

## **Розв'язання задачі технічного захисту інформації за умови впливу "мовоподібної" завади**

*Цирульник С.М., Роптанов В.І., Рехлецький О.С.*

### **Вступ**

Не дивлячись на щонайширше впровадження автоматизованих і комп'ютеризованих систем обробки інформації, людська мова залишається одним з найважливіших шляхів інформаційної взаємодії. Більш того, при децентралізації економічної і політичної системи і відповідному збільшенні частки оперативної інформації, що зв'язує в ухваленні рішень людей, важливість мовного обміну зростає. Одночасно посилюється потреба в забезпеченні конфіденційності мовного обміну.

Захист переговорів, що відбуваються в приміщенні або на контрольованій території завжди вимагає фінансових затрат і може створювати певний дискомфорт для персон, що ведуть переговори.

Суб'єкт, який зацікавлений у захищеному обміні інформацією може обрати наступні шляхи:

- підключення до захищеної державної системи зв'язку;
- організація інформаційного обміну мережами зв'язку загального користування із забезпеченням власними силами захисту від перехоплення або спотворення інформації в каналах зв'язку.

У будь-якому випадку основною задачею є забезпечення захисту інформації від витоку через технічні канали [1].

### **Аналіз останніх досліджень і публікацій**

Захист акустичної (мовної) інформації є однією з найважливіших завдань у загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єкта або установи. Для перехоплення мовної інформації можуть використовуватись широкий арсенал портативних засобів акустичної мовної розвідки, що дозволяють перехоплювати мовну інформацію із прямого акустичного, віброакустичного, електроакустичного й оптико-електронного каналу.

Акустичне маскування ефективно використовується для захисту мовної інформації від витоку по всіх каналах витоку інформаційних сигналів.

Завади типу «білого» шуму реалізовані в більшості існуючих систем і засобів захисту мовної інформації, таких як «ПОРОГ-2М» (НИИСТ МВС РФ), ANG-2000 (Research Electronics, США), VNG-006D (Росія), «Базальт-4 ГА» (Україна), VNG-023 (Росія). Завади типу «кольоровий» шум використовуються в таких системах, як «Кабінет» (Росія), «Барон» (Росія), Ві (Україна). Формування «мовоподібної» завади застосовано у виробках «ЭХО», «Эхо-Кейс» (Росія), ПМ-2А, PSP-2А (Україна), «Mongoose-M» (Україна) [2, 3, 4].

Фахівцями в області технічного захисту інформації В.М. Івановим і А. А. Хоревим запропонований спосіб формування «мовоподібної» завади, що полягає в спеціальному перетворенні приховуваного мовного сигналу за рахунок складної інверсії спектра й акустичної псевдореверберації шляхом множення й ділення його частотних складових і багаторазового накладення прийнятих перевідбитих акустичних сигналів [5]. Запропонований спосіб що реалізовано у виробках «ЭХО», «Эхо-Кейс» [5].

При використанні засобів акустичного захисту виникає дискомфорт, тому актуальними є пристрої, що створюють перешкоду тільки при розмові, в інший же час пристрій «мовчить».

### **Мета дослідження**

Метою дослідження є підвищення захищеності мовної інформації шляхом удосконалення активних методів захисту та технічних засобів на основі сучасної елементної бази.

### **Постановка задачі дослідження**

Провести аналіз методів маскування мовних сигналів та розробити схему пристрою захисту мовної інформації у приміщенні.

## Розв'язання задачі

Для захисту мовної інформації використовують активні і пасивні методи захисту. До пасивних методів захисту відносять створення перешкод, наприклад екранування приладів, звукоізоляція приміщення, використання акустичних екранів та звукопоглинальних матеріалів. Активні методи захисту мовної інформації повинні забезпечувати зменшення співвідношення сигнал/шум за рахунок збільшення рівня шуму.

Найбільш ефективним методом протидії несанкціонованому отриманню мовної інформації є перешкода звукозапису переговорів або її ретрансляції з приміщення шляхом створення шумової акустичної або віброакустичної завади, що забезпечує маскування інформативного сигналу. Співвідношення величини шумового сигналу /величина інформативного сигналу, повинне забезпечувати надійне маскування інформативного сигналу або зниження його розбірливості до допустимих меж.

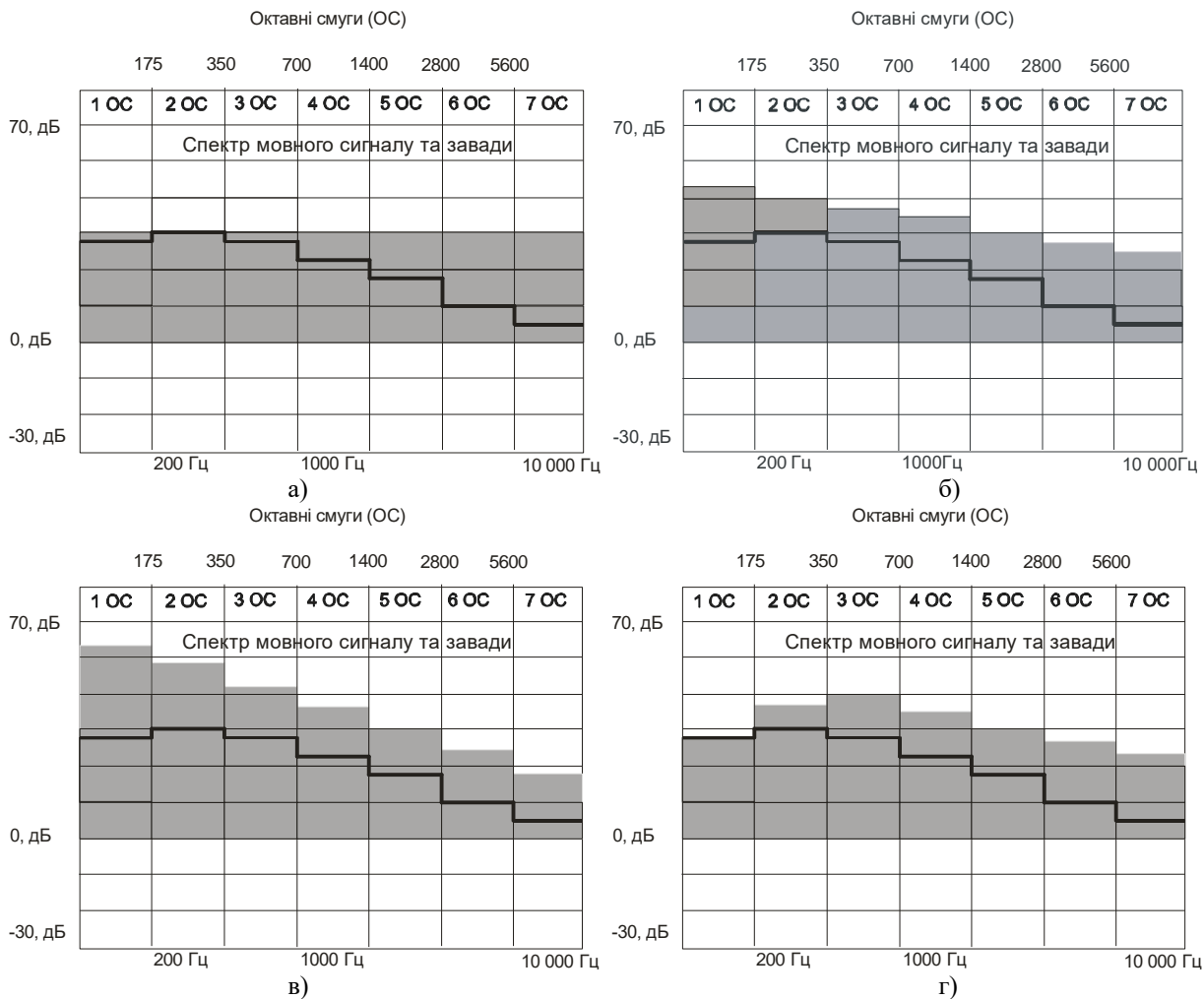


Рисунок 1 – Спектр мовного сигналу та шумової завади: а) «білий» шум, б) «рожевий» шум, в) «коричневий» шум, г) «мовоподібна» завада.

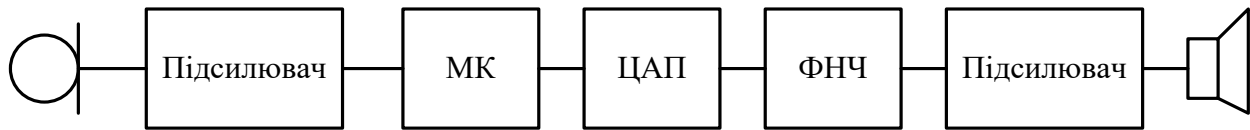
Для захисту мовної інформації використовують такі шумові завади:

- «білий» шум (рисунок 1, а);
- «рожевий» шум (рисунок 1, б);
- «коричневий» шум (рисунок 1, в);
- шумова «мовоподібна» завада (рисунок 1, г).

Співвідношення сигнал/шум між інформативним сигналом та шумоподібними завадами для різної розбірливості мови наведені у таблиці 1.

Аналіз співвідношення сигнал/шум (таблиця 1) показує, що найефективнішим є шумова «мовоподібна» завада та завада типу «рожевий» шум. Для забезпечення необхідного приховування тематики розмови ( $W = 0,2$ ) рівень сигналу завади має перевищувати рівень інформативного сигналу на 8,8 – 9,0 дБ [5-6].

Функціональна схема пристрою, що використовує метод «мовоподібної» завади представлений на рисунку 2.



МК – мікроконтролер, ЦАП – цифро-аналоговий перетворювач, ФНЧ – фільтр нижніх частот

Рисунок 2 – Функціональна схема пристрою захисту мовної інформації методом «мовоподібної» завади.

Прилад розміщується у кімнаті де ведуться переговори. З появою мовного сигналу активізується робота пристрою. Мікроконтролер зчитує цифровий код «мовоподібної» завади, яка попередньо записана до енергонезалежної пам'яті, й передає на цифро-аналоговий перетворювач. До виходу ЦАП підключений фільтр нижніх частот, який усуває завади цифрового перетворення. «Мовоподібна» завада підсилюється і випромінюється гучномовцем або п'єзозвукознімачем. Для створення цифрових даних («мовоподібної завади») використовується персональний комп'ютер з прикладним програмним забезпеченням.

Таблиця 1 – Відношення сигнал/шум для інформативних сигналів при застосуванні шумоподібних завад.

Тип завади	Розбір- ливість мови W,%	Відношення с/ш в октавних смугах					Відношення у смузі частоти 1800-5600 Гц
		250	500	1000	2000	4000	
«Білий» шум	20	0,8	-2,2	-10,7	-18,2	-24,7	-10,0
	30	3,1	0,1	-8,4	-15,9	22,4	-7,7
	40	5,1	2,1	-6,4	-13,9	-20,4	-5,7
«Рожевий» шум	20	-5,9	-5,9	-11,4	-15,9	-19,4	-8,8
	30	-3,7	-3,7	-9,2	-13,7	-17,2	-6,7
	40	-1,9	-1,9	-7,4	-11,9	-15,4	-4,9
«Коричневий» шум Шумова «мовоподібна» завада	20	-14,1	-11,1	-3,6	-15,1	-15,6	-13,0
	30	-12,0	-9,0	-11,5	-13,0	-13,5	-10,8
	40	-10,0	-7,2	-9,7	-11,2	-11,7	-9,0
	20	-3,9	-7,9	-12,9	-15,9	-16,9	-9,0
	30	-1,7	-5,7	-10,7	-13,7	-14,7	-6,8
	40	0,1	-3,9	-8,9	-11,9	12,9	-5,0

Використання мікроконтролера з енергонезалежною пам'яттю дозволяє оперативно змінювати її зміст, що дозволяє більш ефективно здійснювати захист мовної інформації у приміщенні. «Мовоподібним» сигналом можуть бути хибні дані, що попередньо записані від співрозмовників.

Принципіальна схема пристрою приведена на рисунку 3.

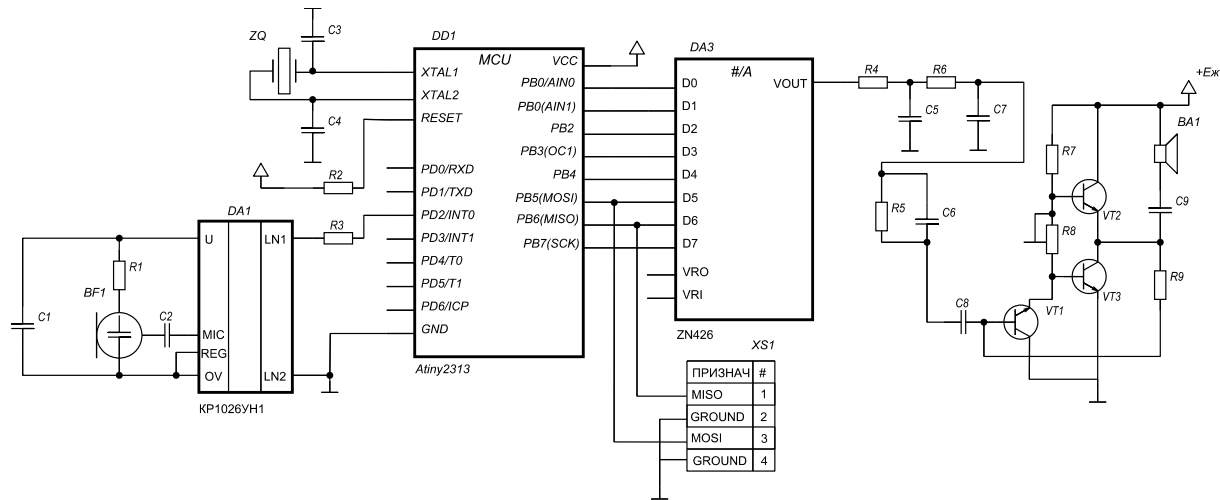


Рисунок 3 – Схема пристрою захисту мовної інформації методом «мовоподібної» завади.

Вхідний каскад, що переводить з енергозберігаючого режиму схему, представляє мікрофонний підсилювач на ІМС KP1026YH1 [7]. Мікроконтролер DD1 типу Atiny2313 фірми Atmel [8]. Через XS1 здійснюється програмування мікроконтролера. На ІМС ZN426 [9] побудований 8-бітний ЦАП з ФНЧ на R4, C5, R6, C7. Вихідний підсилювач виконаний за схемою безтрансформаторного двохтактного підсилювача потужності. Схема вихідного каскаду може змінюватись у залежності від рівня завади.

## Висновки

Проведений аналіз методів маскування мовної інформації показав, що найбільш ефективним є метод захисту «мовоподібною» завадою. Розроблений пристрій використовує зазначений метод й відрізняється від промислових пристроїв мінімальною ціною, можливістю оперативно змінювати зміст «мовоподібною» завади і створювати її тільки під час розмови, що зменшує дискомфорт від застосування засобів акустичного захисту. На базі пристрою можливо побудувати систему протидії технічній розвідці.

## Список літератури

1. Кравченко В. Б. Защита речевой информации в каналах святы/ В. Б. Кравченко // Специальная техника. – 1999. - №4, №5..
2. Офіційна web-сторінка фірми ДЕТЕКТОР SYSTEMS [Електронний ресурс] / Технічні пристрої захисту інформації і системи безпеки.. – Режим доступу: <http://www.detsys.ru/>, вільний. – Загл. з екрана. – Мова рос.
3. Офіційна web-сторінка фірми НЕРА-С [Електронний ресурс] / Разработка и производство средств защиты информации. – Режим доступу: <http://www.nera-s.com/>, вільний. – Загл. з екрана. – Мова рос.
4. Офіційна web-сторінка фірми ТСС [Електронний ресурс] / Техніка для спец. служб – Режим доступу: <http://www.t-ss.ru/>, вільний. – Загл. з екрана. – Мова рос.
5. Халяпин Д. Б. Защита информации. Вас подслушивают? Защищайтесь!/ Д.Б. Халяпин. – М: НОУ ШО «Баярд», 2004 – 432 с. – ISBN 5-94896-017-X
6. Азаров О. Д. Методи і засоби обробки небезпечних сигналів/ О.Д. Азаров, Г.О. Максименко, В.О. Хорошко, Ю.Є. Яремчук. – Вінниця: ВНТУ, 2005. – 282 с.
7. Кизлюк А.И. Справочник по устройству и ремонту телефонных аппаратов зарубежного и отечественного производства/ А.И. Кизлюк. – М: Библион, 1995г. — 191 с..
8. Баранов В. Н. Применение микроконтроллеров AVR: схемы, алгоритмы, программы/ В.Н. Баранов. – М.: Издательский дом «Додэка -XXI», 2004. – 288 с. – ISBN: 5-94120-121-4
9. Микросхемы АЦП и ЦАП. Справочник . — М.: Издательский дом «Додэка-XXI», 2005. — 432 с.

10. Энциклопедия электронных компонентов. Большие интегральные схемы / Под ред. А.Н. Еркина - Т. 1. - М.: ООО «МАКРО ТИМ», 2006. - 224 с. – ISBN: 5-94120-091-9
11. Волович Г. И. Схемотехника аналоговых и аналого-цифровых электронных устройств/ Г.И. Волович. — М.: Издательский дом «Додэка-XXI», 2005. — 528 с. – ISBN 5-94120-074-9
12. Схемотехніка електронних систем: У 3 кн. Кн.2. Цифрова схемотехніка: Підручник / В. І. Бойко, А. М. Гуржій, В. Я. Жуйков та інш. – К.: Вища шк., 2004. – 423 с. – ISBN 966-642-202-6
13. Схемотехніка електронних систем: У 3 кн. Кн.3.Мікропроцесори та мікроконтролери: Підручник / В. І. Бойко, А. М. Гуржій, В. Я. Жуйков та інш. – К.: Вища шк., 2004. – 399с. – ISBN 966-642-202-6

**Цирульник Сергій Михайлович** – к.т.н., відмінник освіти України, голова циклової комісії «Радіотехніка» Вінницького технічного коледжу, svom@list.ru.

**Роптанов Володимир Ілліч** – к.т.н., доцент кафедри обчислювальної техніки, Вінницький національний технічний університет.

**Рехлецький Олександр Станіславович** – студент групи АМЗ-04 факультету комп'ютерних систем та мереж інституту інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, rekhletskey@ukr.net.