[5] Поспелов Д. А. Ситуационное управление: теория и практика / Д. А. Поспелов. – М: Наука, 1986. – 326 с.
[6] Эйкхофф П. Основы идентификации систем управления / П. Эйкхофф. – М: Мир, 1985. – 206с.
[7] Сейдж Э. Теория оценивания и ее применение в связи и управлении. Изд. 3-е доп. / Э. Сейдж, Дж. Мелс. – М: Связь, 2006. – 186 с.
[8] Белецкий В. Н. Многопроцессорные и асинхронные структуры с организацией параллельных вычислений. Изд. 2-е В. / Н. Белецкий – К: Наукова думка, 1998. – 206 с.
[9] Обґрунтування вибору показників оцінки ефективності функціонування автоматизованої системи контролю / В. Кузавков, О. Янковський, Ю. Болотюк // Сучасні інформаційні технології у сфері безпеки та оборони. Розділ: Військова кібернетика та системний аналіз. Том 44, №2. – 2022. – С. 21-27.

TECHNICAL DIAGNOSTICS OF COMPLEX TECHNICAL OBJECTS

The availability of an effective diagnostic system is a necessary condition for the trouble-free functioning of any technical system. However, it should be noted that the cost of development and maintenance of such systems does not allow creating them in mass quantities. The paper proposes a construction option and an algorithm for the functioning of an automated system for solving the problems of technical diagnostics of complex technical objects. The structure of the control system proposed in the work is able to ensure the performance of all tasks of technical diagnostics - control of the technical condition, localization of malfunctions, forecasting of the technical condition of the object of control. The use of computing tools as part of the control system makes it possible to obtain a unified device with a variable structure of both hardware and software components. The thus achieved universality and flexibility of the automated diagnostic system as a device with software control ensures its wide use in systems of technical diagnostics and control of complex objects.

Keywords: technical condition, control system, technical diagnostics, control object, complex technical object.

Кузавков Василь Вікторович, доктор технічних наук, доцент, начальник кафедри побудови телекомунікаційних систем Військового інституту телекомунікацій та інформатизації імені Героїв Крут.

Vasyl Kuzavkov, doctor of technical sciences, associate professor, the head of the department of construction of telecommunication systems of the Military Institute of Telecommunications and Informatization named after the Heroes of Kruty.
E-mail: nevse@ukr.net.
Orcid ID: 0000-0002-0655-9759.

Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Volodymyr Khoroshko, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

Янковський Олег Георгійович, кандидат технічних наук, доцент, доцент кафедри телекомунікаційних систем та мереж Військового інституту телекомунікацій та інформатизації імені Героїв Крут.

Oleg Iankovskii, candidate of technical sciences, associate professor, associate professor department of telecommunication systems and networks of the Military Institute of Telecommunications and Informatization named after the Heroes of Kruty.
E-mail: yankovsky@onua.edu.ua.
Orcid ID: 0000-0001-8041-1843.

DOI: 10.18372/2410-7840.24.17189
УДК 004.056

ДИФЕРЕНЦІАЛЬНИЙ СПЕКТР МОВНОЇ ІНФОРМАЦІЇ

Ольга Грищук

В умовах повсюдної доступності комунікаційних систем кожен з абонентів інформаційного обміну здебільшого прагне досягнути максимальної конфіденційності під час спілкування. Для задоволення цієї потреби у світі розроблено та впроваджено низку новітніх технологій захисту мовної інформації. Наприклад, відомі найпростіші програмні, апаратні та програмно-апаратні засоби захисту мовної інформації у вигляді скремблерів або більш новітні програмні засоби потокового шифрування в загальнодоступних месенджерах WhatsApp, Signal тощо. Засоби криптографічного захисту мовної інформації також широко використовуються в таких радіостанціях, як Motorola, Hytera та ін. Питання забезпечення конфіденційності мовної інформації в комунікаційних системах спеціального призначення взагалі є однією з ключових вимог, яка висувається до систем такого типу. Незважаючи на застосовувані технології забезпечення конфіденційності

мовної інформації кількість спроб несанкціонованого доступу до неї постійно зростає, тому порушена проблема є актуальною. У статті, ґрунтуючись на попередніх відомих дослідженнях, запропоновано подати мовну інформацію у вигляді диференціального спектра в основу якого покладено її гармонічну модель. Диференціальний спектр мовної інформації отримується на основі диференціальних перетворень академіка НАН України Г. Пухова. Для забезпечення заданої точності відновлення мовної інформації в режимі реального часу було обґрунтовано мінімально необхідну кількість дискрет диференціального спектра. Показано й доведено, що диференціальний спектр мовної інформації є підґрунтям для використання його в альтернативній системі шифрування мовної інформації з гарантованою криптостійкістю – криптографічній системі Фредгольма. Отримані результати можуть бути узагальнені для дослідження диференціальних спектрів мовної інформації, поданої й іншими моделями, відмінними від гармонічної.

Ключові слова: *диференціальний спектр, мовна інформація, дискрета, цілочисловий аргумент, перетворення, гармонічна модель.*

ВСТУП

У світлі останніх подій в Україні питання забезпечення кібербезпеки в цілому [1, 2] та кіберзахисту зокрема [3] суттєво актуалізується. З усієї множини безпекових проблем особливо гостро стоїть проблема криптографічного захисту мовної інформації [4, 5], яка циркулює в комунікаційних системах різного цільового призначення. Суттєве зростання кількості кібератак [6] за останнє десятиліття [7] та нарощення їх технологічної складності значно загострює означену проблему. Наразі є потреба в пошуку нових нетривіальних підходів до забезпечення безпеки мовної інформації, адже успішне вирішення зазначеної проблеми сприятиме запобіганню багатьох кіберінцидентів і гарантуватиме учасникам інформаційного обміну конфіденційність у вирішенні широкого спектра питань міжособистісного спілкування.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Мовна інформація, що підлягає криптографічному захисту, як випливає з результатів аналізу останніх досліджень і публікацій за визначеною темою, може бути описана низкою математичних моделей. Проаналізувавши їх, можна виокремити два типові класи.

Перший клас математичних моделей мовної інформації – це динамічні математичні моделі. В їх основу, як випливає з [8], покладено моделі, розроблені на основі вейвлет-коефіцієнтів, імпульсно-модульованих сигналів, хвильових рівнянь, гармонічних сигналів тощо. Другим широким класом математичних моделей мовної інформації є стохастичні моделі, які, як показано в [9–12], базуються на прихованих марковських моделях та стохастичних моделях на основі *"on/off"* послідовностей тощо.

Проте незважаючи на значну кількість динамічних та стохастичних моделей, на сьогодні й досі не розроблено диференціальних спектрів мовної інформації, які можуть бути використані в перспективних криптографічних системах [13].

МЕТА ДОСЛІДЖЕННЯ

Метою статті є побудова й дослідження диференціального спектра мовної інформації для подальшого його використання в прикладних задачах криптографічного захисту в комунікаційних системах з підвищеними вимогами до забезпечення конфіденційності.

РЕЗУЛЬТАТИ ТА ЇХ ОБГОВОРЕННЯ

У [13] вперше висунуто ідею використання алгебричної методології для побудови криптографічних систем нового покоління. Разом з тим ні в [13], ні в інших наукових працях не запропоновано криптографічного протоколу для її реалізації.

З метою практичної реалізації запропонованої в [13] методології в [14] детально описано послідовність процедур шифрування та розшифрування. У [15] висунуто вимоги до ключа шифрування, а в [16] наведено приклад його вибору відповідно до висунутих вимог. Наступним кроком має бути вибір моделі мовної інформації та побудова її диференціального спектра.

На сьогодні найбільш розповсюдженим класом моделей, про які мова йшла вище, є гармонічні математичні моделі мовної інформації. Це обумовлено низкою їх переваг порівняно з іншими відомими моделями. Вони мають високий ступінь адекватності, що досягається унаслідок декомпозиції гармонічного сигналу на періодичну (вокалізовану) і шумову та/або завадову (невокалізовану) складові. Тому для побудови диференціального спектра мовної інформації на основі обраного класу моделей здійснимо аналіз та синтез вихідної гармонічної математичної моделі мовної інформації.

Аналіз вихідної гармонічної математичної моделі мовної інформації. Нехай у мовному сигналі $z(t)$, який передається в реальній комунікаційній системі, присутня суміш періодичної складової мов-

ної інформації $h(t)$ разом з мультиплікативною $\delta(t)$ й адитивною $r(t)$ завадами, тобто

$$z(t)=\delta(t)h(t)+r(t). \quad (1)$$

Проаналізуємо спотворення мовного сигналу (1), обумовлені наявністю в ньому мультиплікативної та адитивної завад.

Мультиплікативна завада $\delta(t)$ спричинена випадковими змінами параметрів каналу зв'язку. Зокрема, для радіоканалу джерелом таких завад можуть бути неоднорідності середовища поширення радіохвиль. Прояв мультиплікативних завад, як правило, зводиться до зміни рівня (амплітуди і, відповідно, потужності) мовного сигналу $z(t)$. У реальних умовах мультиплікативна завада $\delta(t)$ описується моделлю випадкового процесу та компенсується з використанням відомого методу гомоморфної фільтрації [17]. Отже, застосування методу гомоморфної фільтрації дозволяє компенсувати спотворення мовної інформації, зумовлені наявністю в ньому мультиплікативної завади.

Адитивна завада $r(t)$ мовного сигналу (1) є стаціонарним випадковим процесом із нормальним законом розподілу, який на практиці найчастіше являє собою флуктуаційний шум радіоефіру. З метою виділення із суміші мовного сигналу мовної інформації адитивна завада компенсується за рахунок віднімання її від сигналу, що спостерігається. Іншим альтернативним підходом є застосування методів адаптивної фільтрації. Отже, як у першому, так і в другому випадках сутність компенсації адитивної завади зводиться до її фільтрації [18].

У результаті попередньої селекції мовного сигналу $z(t)$ (1) й фільтрації його від мультиплікативної $\delta(t)$ та адитивної $r(t)$ завад його періодична складова, яка є мовною інформацією $h(t)$, може бути описана гармонічною моделлю загального вигляду, що є деяким модульованим коливанням:

$$h(t)=A_m(t)\cos\psi_m(t), \quad (2)$$

де $A_m(t)$ – миттєва амплітуда мовної інформації в деякий момент часу t; $\psi_m(t)$ – повна миттєва фаза мовної інформації в той самий момент часу t. Слід зазначити, що в моделі (2) $A_m(t)$ та $\psi_m(t)$ є інформаційними параметрами мовної інформації, яка передається.

Синтез вихідної гармонічної математичної моделі мовної інформації. На сьогодні з усієї множини гармонічних сигналів (2) з аналоговою модуляцією в системах радіозв'язку в УКХ діапазоні частот для передачі мовної інформації найбільш часто застосовуються сигнали з кутовою (частотною або фазовою) модуляцією. Математична модель такого сигналу без завад, як випливає з [19], й моделі (2), за умов

$$A_m(t)\Rightarrow A_m,\ A_m=const;$$
$$\psi_m(t)=2\pi f_m t+\varphi_m(t)+\varphi_m,$$

у загальному вигляді зводиться до виразу

$$h(t)=A_m\cos\left(2\pi f_m t+\varphi_m(t)+\varphi_m\right), \quad (3)$$

де A_m – амплітуда, f_m – циклічна частота, $\varphi_m(t)$ – фазова функція, φ_m – початкова фаза мовної інформації.

На сьогодні серед усіх відомих видів кутової модуляції під час організації радіозв'язку, особливо в системах спеціального призначення [20], найбільш часто як математична модель мовної інформації використовується вузькосмугова частотна модуляція (*Narrowband frequency modulation – NBFM*) [21]. Такий вид модуляції достатньо стійкий до завад та погодних умов, що є його перевагою. Застосування вузькосмугової частотної модуляції, за умови $\varphi_m=0$, після тривіальних математичних перетворень дозволяє синтезувати гармонічну математичну модель мовної інформації таким виразом:

$$h_{NBFM}(t)\cong A_c\cos\left(2\pi f_c t\right)-\frac{A_c\beta}{2}\times$$
$$\times\cos\left(2\pi\left(f_c-f_m\right)t\right)+\frac{A_c\beta}{2}\times \quad (4)$$
$$\times\cos\left(2\pi\left(f_c+f_m\right)t\right),$$

де A_c – амплітуда, f_c – циклічна частота несучого коливання, β – індекс кутової модуляції, $\beta\le 1$. У виразі (4) для подальшого спрощення математичних викладок прийнято вважати рівними нулю початкові фази для несучого коливання φ_c та мовної інформації φ_m, тобто $\varphi_c=0$ та $\varphi_m=0$. Отже, опираючись на викладені вище твердження модель (4) вважаємо вихідною для побудови диференціального спектра мовної інформації.

Диференціальні перетворення гармонічної математичної моделі мовної інформації. Для побудови диференціального спектра мовної інформації пропонуємо скористатися операційним методом диференціальних перетворень академіка НАН України Г. Пухова [22]. Однією з його численних переваг є

можливість отримання аналітичних моделей диференціальних спектрів фізичних процесів різної природи, які описуються трансцендентними функціями без втрат точності вихідної математичної моделі. Трансцендентна природа вихідної математичної моделі зводиться до простих арифметичних операцій над її диференціальними спектрами, що в подальшому суттєво спрощує практичну реалізацію засобів криптографічного захисту інформації.

Згідно з [22] диференціальні перетворення передбачають подання вихідної математичної моделі степеневим рядом Тейлора з центром у точці $t=0$. Пряме і, відповідно, зворотне перетворення мають такий вигляд:

$$X(k)=\underline{x}(k)=\frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \;\underline{\cdot}\!\!\circ\; x(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k X(k), \quad (5)$$

де $x(t)$ – оригінал, який є безперервною, що диференціюється нескінченну кількість разів, і обмежену разом з усіма своїми похідними функцію дійсного аргументу t; $X(k)$ і $\underline{x}(k)$ – рівноцінні позначення диференціального зображення оригіналу, що описує дискретну (гратчасту) функцію цілочислового аргументу $k=0,1,2,...$; H – масштабна стала, яка має розмірність аргументу t і часто обирається рівною відрізку $0\le t\le H$, на якому розглядається функція $x(t)$; $\underline{\cdot}\!\!\circ$ – символ відповідності між оригіналом $x(t)$ і його диференціальним зображенням $X(k)=\underline{x}(k)$. Згідно з (5) пряме перетворення дозволяє за оригіналом $x(t)$ знайти зображення $X(k)$, а зворотне перетворення (праворуч від символу $\underline{\cdot}\!\!\circ$) дозволяє за зображенням $X(k)$ отримати оригінал $x(t)$. Диференціальні зображення $X(k)$ називаються диференціальними *Т-спектрами*, а значення *Т-функції* $X(k)$, за конкретних значень аргументу k – дискретами.

Скориставшись прямим диференціальним перетворенням (5), в області зображень гармонічну математичну модель мовної інформації, що описується вузькосмуговим частотно-модульованим сигналом (4), можна записати в такому вигляді:

$$H_{NBFM}(k)=A_c\left(\frac{2\pi f_c H}{k!}\right)^k\cos\left(\frac{\pi k}{2}\right)-$$
$$-\frac{A_c\beta}{2}\left(\frac{2\pi(f_c-f_m)H}{k!}\right)^k\cos\left(\frac{\pi k}{2}\right)+ \quad (6)$$
$$+\frac{A_c\beta}{2}\left(\frac{2\pi(f_c+f_m)H}{k!}\right)^k\cos\left(\frac{\pi k}{2}\right),$$

де $\left(\frac{2\pi f_c H}{k!}\right)^k\cos\left(\frac{\pi k}{2}\right)$ – Т-косинус, який описує мовну інформацію на несучій частоті f_c; $\frac{A_c\beta}{2}\left(\frac{2\pi(f_c-f_m)H}{k!}\right)^k\cos\left(\frac{\pi k}{2}\right)$ – Т-косинус, який описує мовну інформацію на нижній боковій частоті f_c-f_m; $\frac{A_c\beta}{2}\left(\frac{2\pi(f_c+f_m)H}{k!}\right)^k\cos\left(\frac{\pi k}{2}\right)$ – Т-косинус, який описує мовну інформацію на верхній боковій частоті f_c+f_m.

Побудуємо диференціальний спектр мовної інформації (6), скориставшись прямим диференціальним перетворенням (5). З [22] відомо, що для зображень, які описуються Т-косинусами, найбільш інформативними є перші п'ять дискрет диференціального спектра. Знайдемо їх, послідовно змінюючи значення цілочислового аргументу k від 0 до 4, тобто $k=0...4$.

Для цілочислового аргументу $k=0$ нульова дискрета набуватиме такого вигляду:

$$H_{NBFM}(0)=A_c. \quad (7)$$

Наступні чотири дискрети диференціального спектра мовної інформації відповідно дорівнюватимуть:

для $k=1$

$$H_{NBFM}(1)=0; \quad (8)$$

для $k=2$

$$H_{NBFM}(2)=-2A_c\pi^2 f_c^2 H^2+$$
$$+A_c\beta\pi^2(f_c-f_m)^2H^2-$$
$$-A_c\beta\pi^2(f_c+f_m)^2H^2=$$
$$=-2A_c\pi^2 f_c H^2(f_c+2\beta f_m); \quad (9)$$

для $k=3$

$$H_{NBFM}(3)=0; \quad (10)$$

для $k=4$

$$H_{NBFM}(4)=\frac{2}{3}A_c\pi^4 f_c{}^4H^4-$$
$$-\frac{1}{3}A_c\beta\pi^4\left(f_c-f_m\right)^4H^4-$$
$$-\frac{1}{3}A_c\beta\pi^4\left(f_c+f_m\right)^4H^4=$$
$$=\frac{2}{3}A_c\pi^2 f_cH^4\left(f_c{}^3+4\beta f_m\left(f_c{}^2+f_m{}^2\right)\right). \quad (11)$$

Отже, шуканий диференціальний спектр мовної інформації (4) описується набором дискрет (7), (9) та (11), оскільки дискрети (8) та (10) дорівнюють нулю.

Експериментальна перевірка отриманих результатів

1. Обґрунтування параметрів вихідної гармонічної моделі мовної інформації.

1.1. Обґрунтування вибору частотного діапазону модулюючого коливання f_m.

Загальновідомо, що частотний діапазон мовної інформації коливається в межах від 70 Гц до 7 кГц. Семантична (змістовна) складова мовної інформації у визначеному діапазоні змінюється в межах від 200 Гц до 5 кГц, а вокалізована – від 80 Гц до 2,5 кГц. Графічне подання зазначених діапазонів на рис. 1 дозволяє обґрунтовано обрати частотний діапазон для модулюючого коливання.

Так, з результатів аналізу перекриття частотних діапазонів, наведених на рис. 1, випливає, що за частотний діапазон модулюючого коливання f_m доцільно обрати діапазон від 200 Гц до 2,5 кГц.

Цей діапазон, по-перше, є мовним; по-друге, містить семантичну складову мовної інформації; по-третє, мовна інформація включає лише вокалізовану (періодичну) складову.

1.2. Обґрунтування вибору частоти несучого коливання f_c.

Нехай частота несучого коливання f_c відповідає робочому діапазону частот будь-якої з широко застосовуваних на сьогодні радіостанцій, наприклад, радіостанції *RF-7800H-MR* фірми *"HARRIS"* сімейства *FALCO III*. В УКХ діапазоні цієї радіостанції частотно-модульований сигнал випромінюється на частотах від 20 МГц до 59,9999 МГц [23].

1.3. Вибір амплітуди несучого коливання A_c.

Для згаданої вище радіостанції на мінімальній потужності випромінювання вихідного сигналу в 1 Вт амплітуда несучого коливання приймається рівною 7 В.

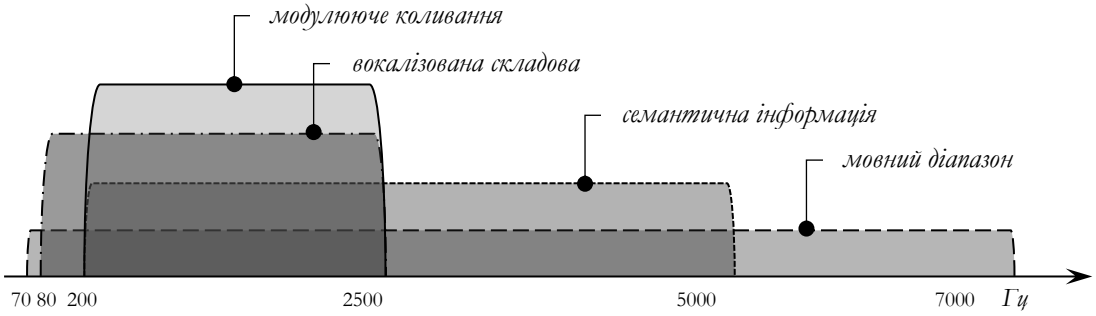


Рис. 1. Графічний спосіб обґрунтування вибору частотного діапазону модулюючого коливання f_m

1.4. Девіація частоти Δf для вузькосмугових частотно-модульованих сигналів не повинна перевищувати 5 кГц.

1.5. Індекс кутової модуляції обирається, виходячи з необхідності забезпечення

1.6. Ширина смуги пропускання B_T обирається за емпіричним правилом Карсона й для кращого прийому визначається як $B_T=2f_m(\beta+1)$, що свідчить про наявність 98% енергії сигналу в її межах. Отже, вихідна гармонічна математична модель мовної інформації (4), параметри якої обрані відповідно до пунктів 1.1–1.6, матиме такий вигляд:

$$h_{NBPM}(t)=7\cos\left(2\pi 45\times10^6 t\right)-$$
$$-0,35\cos\left(2\pi\left(45\times10^6-700\right)t\right)+ \quad (12)$$
$$+0,35\cos\left(2\pi\left(45\times10^6+700\right)t\right),$$

де

$$\begin{cases} f_m=700\,Гц; \\ f_c=45\times10^6\,Гц; \\ A_c=7\,В; \\ \Delta f=70\,Гц; \\ \beta=0,1; \\ B_T=1540\,Гц. \end{cases}$$

2. Експериментальна установка.

Склад експериментальної установки для дослідження характеристик мовного сигналу в часовій і спектральних областях зібрано з метою перевірки адекватності синтезованої вихідної гармонічної математичної моделі мовної інформації (4) та її окремих випадків, наприклад, (12). До складу експериментальної установки включено:

- генератор сигналів *SIGLANT SDG 2122 X*, призначений для генерування несучого й модулюючого коливань та формування вузькосмугового частотно-модульованого сигналу *NBFM* (4) і його окремих випадків (12);
- осцилограф *SIGLANT SDG 1202X-E*, призначений для одночасного дослідження частотно-модульованого сигналу *NBFM* та його складових: несучого й модулюючого коливань у часовій області;
- аналізатор спектра RIGOL DSA 815, призначений для дослідження спектра вузькосмугового частотно-модульованого сигналу *NBFM*.

Конфігурацію устаткування для дослідження синтезованої моделі (12) наведено на рис. 2.

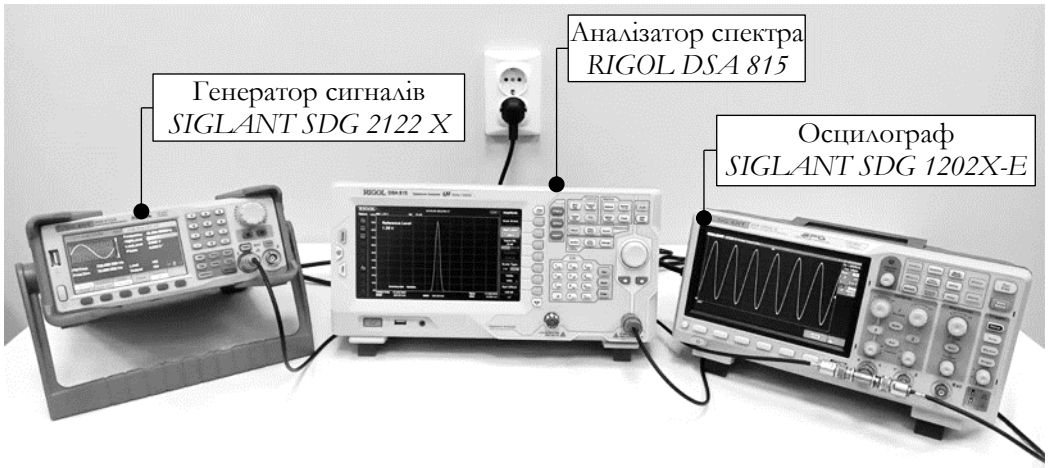
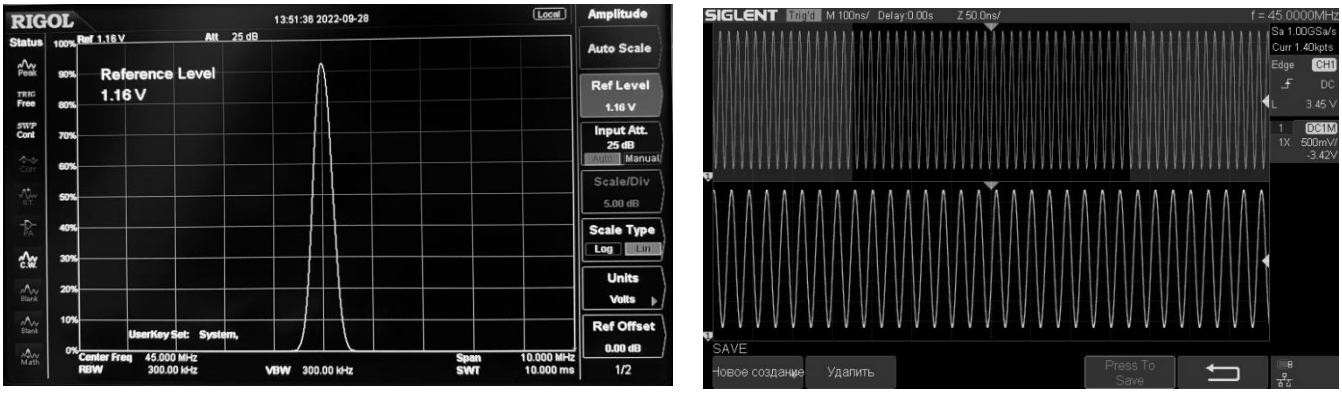


Рис. 2. Схема експериментальної установки для дослідження моделі мовної інформації

На рис. 2 усі пристрої експериментальної установки є цифровими, що забезпечує високу стабільність і точність параметрів досліджуваної моделі.

Візуалізація отриманих результатів

На рис. 3 наведено спектральні та часові графіки досліджуваної моделі, отримані за допомогою зібраної експериментальної установки.



а) б)

Рис. 3. Графіки вузькосмугового частотно-модульованого сигналу $h_{NBPM}(t)$:
а – амплітудно-частотний спектр; б – осцилограма сигналу з різним періодом часової розгортки

Отже, для обраних параметрів моделі (12) отримані результати візуалізації (див. рис. 3) повністю відповідають відомим характеристикам вузькосмугових частотно-модульованих сигналів [24]. Із отриманих результатів випливає, що вихідна математична модель (4) є адекватною, а це дозволяє використовувати її для побудови диференціального спектра мовної інформації.

3. Побудова диференціального спектра мовної інформації.

Опираючись на обґрунтування параметрів вихідної гармонічної математичної моделі, побу-

дуємо диференціальний спектр мовної інформації (7), (9) та (11), перейшовши від його аналітичного вигляду (6) до числового подання.

На основі обґрунтованих у п. 1 параметрів моделі мовної інформації вона зводиться до такого вигляду:

$$H_{NBFM}(k) = 7\left(\frac{2\pi 45\times 10^6 H}{k!}\right)^k \cos\left(\frac{\pi k}{2}\right) - $$
$$-0,35\left(\frac{2\pi(44999300)H}{k!}\right)^k \cos\left(\frac{\pi k}{2}\right) + \qquad (13)$$
$$+0,35\left(\frac{2\pi(45000700)H}{k!}\right)^k \cos\left(\frac{\pi k}{2}\right).$$

Взявши отриману модель за основу та опираючись на (7), (9) й (11), подамо диференціальний спектр мовної інформації як

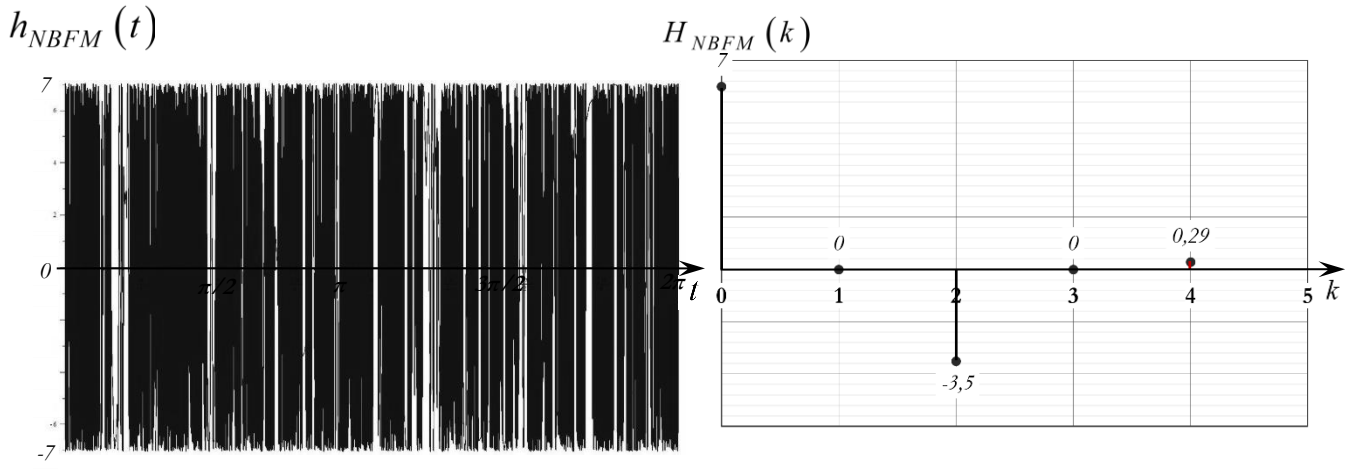
$$k := 0,...,4 \Rightarrow \begin{cases} H_{NBFM}(0) = 7; \\ H_{NBFM}(1) = 0; \\ H_{NBFM}(2) = -3,5; \\ H_{NBFM}(3) = 0; \\ H_{NBFM}(4) = 0,29, \end{cases} \qquad (14)$$

за умови, що масштабна стала $H = \frac{1}{2\pi f_c}$, тобто $H = 3,54$ нс. Графічну візуалізацію диференціального спектра мовної інформації наведено на рис. 4 б, а на рис. 4 а для порівняння надано його форму в часовій області, отриману за допомогою засобів графічного дизайну системи аналітичної математики *Maple*.

Отже, мовна інформація, яка описується гармонічною математичною моделлю (4) та є вузькосмуговим частотно-модульованим сигналом, у часовій та частотних областях подається за допомогою диференціальних перетворень в області зображень диференціальним спектром (7), (9) та (11), дискрети якого є набором чисел за конкретних числових значень параметрів моделі. Кількість дискрет диференціального спектра мовної інформації визначає точність відновлення мовної інформації в області оригіналів і на практиці обмежується першими чотирма дискретами. З рис. 4 видно, що подальші процедури шифрування в криптографічній системі Фредгольма [14] зведуться до арифметичних операцій над числами, які легко реалізуються відомими апаратними, програмно-апаратними та програмними криптографічними засобами захисту мовної інформації [25].

ВИСНОВКИ

У результаті проведеного дослідження обґрунтовано модель мовної інформації та вперше в аналітичному вигляді отримано її диференціальний спектр. Адекватність отриманої моделі доведено експериментально шляхом порівняння вихідної математичної моделі з даними відомих досліджень.



а) б)

Рис. 4. Мовна інформація (а) та її диференціальний спектр (б)

Збіжність параметрів вихідної математичної моделі мовної інформації яка описується вузькосмуговим частотно-модульованим сигналом, дозволила зробити висновок про адекватність отриманого її диференціального спектра. Напрямком подальших досліджень є розроблення протоколу шифрування в криптографічній системі Фредгольма на основі отриманого диференціального спектра.

ЛІТЕРАТУРА

[1] Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник; за заг. ред.

проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

[2] Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир : ЖНАЕУ, 2019. – 280 с.

[3] Serpanos D. The Cyberwarfare in Ukraine / D. Serpanos and T. Komninos // Computer. – 2022. – Vol. 55, No. 7. – pp. 88–91.

[4] Kumar L. P. Implementation of speech encryption and decryption using advanced encryption standard / L. P. Kumar, A. K. Gupta // 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTE ICT). – 2016. – pp. 1497–1501.

[5] [5] El Assad S. Special Issue on Cryptography and Its Applications in Information Security / S. El Assad, R. Lozi, W. Puech // Applied Sciences. – 2022. – Vol. 12 (No. 5). – pp. 1-3.

[6] Мальцева І. Р. Аналіз деяких кіберзагроз в умовах війни / І. Р. Мальцева, Ю. О. Черниш, Р. М. Штонда // Кібербезпека: освіта, наука, техніка. – 2022. – Вип. 4 (№ 16). – С. 37-44.

[7] Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах / Р. В. Грищук/ / Сучасна спеціальна техніка. – 2011. – № 1. – С. 61-66.

[8] Голубинский А. Н. Математическая модель речевого сигнала, основанная на аппроксимации спектра набором постоянных составляющих в соответствующих полосах частот / А. Н. Голубинский // Безопасность информационных технологий. – 2009. – № 2. – С. 12-18.

[9] Применение современных технологий распознавания речи при создании лингвистического тренажера для повышения уровня языковой компетенции в сфере межукультурной коммуникации / Д. С. Колесникова, А. К. Рудниченко, Е. А. Верещагина и др. // Интернет-журнал "Науковедение". – 2017. – Т. 9 (№ 6). – С. 1-12.

[10] Грачев А. М. Статистические подходы к автоматическому распознаванию речи / А. М. Грачев // Вестник Нижегородского университета им. Н. И. Лобачевского. – 2015 – № 2 (2). – С. 376-379.

[11] [11] Bryan J. D. Autoregressive Hidden Markov Model and the Speech Signal / J. D. Bryan, S. E. Levinson // Procedia Computer Science. – 2015. – № 61. – pp. 328-333.

[12] Огнев И. В. Распознавание речи методами скрытых марковских моделей в ассоциативной осцилляторной среде / И. В. Огнев, П. А. Парамонов // Технические науки. Информатика, вычислительная техника. – 2013. – С. 115-126.

[13] Криптография нового поколения: Интегральные уравнения как альтернатива алгебраической методологии / Г. К. Броншпак, И. А. Громыко, С. И. Доценко, Е. А. Перчик // Прикладная электроника. – 2014. – Т. 13, №3. – С. 337–349.

[14] Грищук Р. В. Узагальнена модель криптосистеми Фредгольма / Р. В. Грищук, О. М. Грищук // Кібербезпека: освіта, наука, техніка. – 2019. – № 4. – С. 14–23.

[15] Грищук О. М. Особливості вибору ключа шифрування для криптосистеми Фредгольма / О. М. Грищук // Комп'ютерна інженерія і кібербезпека: досягнення та інновації: матеріали II Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених – Кропивницький : ЦНТУ, 2020. – С. 109-110.

[16] Hryshchuk O. Spectral Model of the Encryption Key for a Symmetric Cryptosystem Based on Differential Transformations / O. Hryshchuk // III International Scientific and Practical Conference "Information Security and Information Technologies", September 13-19, 2021, Odesa, Ukraine. – pp. 218-222.

[17] Панько С. П. Радиотехнические системы специального назначения. Системы связи / С. П. Панько, Е. Н. Гарин, В. В. Сухотин. – Красноярск: СФУ, 2019. – 340 с.

[18] Hansler E. Topics in acoustic echo and noise control: Selected methods for the cancelation of acoustic echoes, the reduction of background noise, and speech processing / E. Hansler, G. Schmidt. – Berlin; Heidelberg: Springer, 2006. – 642 p.

[19] Азаров А. С. Вычисление мгновенных гармонических параметров речевого сигнала / И. С. Азаров, А. А. Петровский // Речевые технологии. – 2008. – № 1. – С. 67-77.

[20] Satellite communications DOD: Should Explore Options to Meet User Needs for Narrowband Capabilities [Електронний ресурс] // United States Government Accountability Office. – 2021. – Режим доступу до ресурсу: https://www.gao.gov/assets / gao-21-105283.pdf.

[21] Rogozinsky G. Some New Mathematical Models of Synthesized Sound Signals / G. Rogozinsky, M. Chesnokov, A. Kutlyiarova // Труды учебных заведений связи. – 2022. – С. 76-81.

[22] Пухов Г. Э. Дифференциальные спектры и их модели. – К.: Наук. думка, 1990. – 184 с.

[23] Лаврут О. О. Перспективи розвитку автоматизованих систем управління тактичної ланки управління Сухопутних військ Збройних Сил України / О. О. Лаврут, О. К. Климович, Т. В. Лаврут // Системи обробки інформації. – 2014. – Вип. 5 (121). – С. 116-120.

[24] Павлюк В. В. Програмно визначене радіо. Вигляд із середини / В. В. Павлюк. – Житомир: Вид. О. О. Євенок, 2021. – 680 с.

[25] Ленков С. В. Методы и средства защиты информации: в 2-х т. / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К.: Арий, 2008. – Т. II. Информационная безопасность. – 344 с.

DIFFERENTIAL SPECTRUM OF SPEECH INFORMATION

In the conditions of widespread availability of communication systems, each of the subscribers of information exchange in most cases seeks to achieve maximum confidentiality during mutual communication. To meet this need, a number of the latest technologies for the protection of speech information have been developed and implemented in the world. For example, the simplest software and hardware means of protecting speech information in the form of scramblers are known, or more advanced software means of stream encryption in public messengers WhatsApp, Signal, etc. Means of cryptography security of speech information are also widely used in radio stations such as Motorola, Hytera, etc. The issue of ensuring the confidentiality of speech information in special purpose communication systems is one of the key requirements for such type systems. Despite the technologies used to ensure the confidentiality of speech information, the number of attempts to gain unauthorized access to it is constantly increasing, so the issue of ensuring its security is currently relevant. In this article, on the basis of previously known research, it is proposed to present speech information in the form of a differential spectrum based on its harmonic model. The differential spectrum of speech information is obtained on the basis of differential transformations of Academician of the National Academy of Sciences of Ukraine H. Pukhov. To ensure the given precision of speech information restoration in real time, the minimum required number of differential spectrum discretes was substantiated. It is shown and proven that the differential spectrum of speech information considered in the article is the basis for its use in an alternative system of encryption of speech information with guaranteed cryptographic resistance - the Fredholm's cryptosystem. The obtained results can be generalized to gain differential spectrums of speech information, provided by other models, other than the harmonic model considered in the article.

Key words: differential spectrum, speech information, discrete, integer argument, transformation, harmonic model.

Грищук Ольга Михайлівна, аспірантка кафедри безпеки інформаційних технологій Національного авіаційного університету.

Olha Hryshchuk, PhD student of the department of security of information technologies of the National Aviation University.
E-mail: Ol.Hry@i.ua.
Orcid ID: 0000-0001-6957-4748.

DOI: 10.18372/2410-7840.24.17264

УДК 004.056.53:534.4

УДОСКОНАЛЕННЯ МЕТОДУ ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМ ВИЯВЛЕННЯ СИГНАЛІВ ЗАСОБІВ НЕГЛАСНОГО ЗДОБУТТЯ ІНФОРМАЦІЇ

Олександр Лаптєв, Віталій Савченко, Віталій Пономаренко,

Сергій Копитко, Іван Пархоменко

В процесі виявлення та розпізнавання сингалів випадкових сигналів, які можуть бути сигналами цифрових засобів негласного здобуття інформації актуальним питанням є підвищення завадостійкості. У статті досліджено особливості застосування фільтрів низької частоти. Фільтрів низької частоти з квадратичною та лінійною залежністю відгуку від вхідного сигналу. Принцип роботи фільтрів полягає у тому, що виконується процес підсумовування. При цьому, корисний сигнал підсумовується когерентне, а сигнал завади – некогерентне. Корисний сигнал збільшується, а сигнал завади зменшується. Під час подачі на вхід лінійного та квадратичного фільтрів прямокутного імпульсу, який імітує сигнали сучасних цифрових засобів негласного здобуття інформації, визначені необхідні для подальшого використання параметри вихідних сигналів: математичне сподівання, коефіцієнт кореляції, дисперсія, середньоквадратичне відхилення, відношення величини сигналів до величини завад у часовому та спектральному вигляді. Обчислено коефіцієнт виграшу. Цей коефіцієнт показує ефективність використання фільтрів низької частоти. Наведено графіки огинаючої напруги на виході ідеального смугового фільтру при поданні на вхід прямокутного імпульсу з різною тривалістю – сигналу, якій може бути сигналом засобів негласного здобуття інформації. Проведено моделювання процесу фільтрації при різних коефіцієнтах кореляції. Результати моделювання підтвердили можливість виділення сигналу засобів негласного здобуття інформації методом визначення двомірної щільності ймовірності сигналу завади на фоні загального сигналу. Досліджується процес підвищення завадостійкості системи у цілому. Удосконалення методу виявлення сигналів проведено за рахунок використання у процесі обробки сигналів вузькосмугових фільтрів низької частоти, що дозволяє досягти підвищення завадостійкості системи визначення та розпізнавання сигналів цифрових засобів негласного здобуття інформації на 23 %.