Зв'язок, радіотехніка, радіолокація, акустика та навігація

УДК 681.324 DOI: 10.30748/zhups.2019.60.10

А.Е. Бекіров, О.М. Баранік, В.В. Парфило

Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків

МЕТОД ПРИХОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ В МОВНОМУ ПОВІДОМЛЕННІ

В статті розглядається актуальне питання функціонування системи інформаційної підтримки виконання бойових завдань екіпажами повітряних суден. Аналізуються зразки існуючого вітчизняного та закордонного обладнання обміну інформаційними повідомленнями. Для усунення виявлених обмежень щодо функціонування розглянутого обладнання в єдиному інформаційному просторі пропонується напрямок, який передбачає маскування даних в мовних повідомленнях з подальшою передачею в аналогових радіостанціях. Сформовано вимоги до алгоритму, які полягають у мінімізації спотворень вихідного голосового повідомлення в результаті вбудовування інформації. Розроблено метод маскування даних в мовних повідомленнях на основі модифікації фаз фрагментів за непрямим правилом. На основі програмної моделі проведено оцінку розробленого методу.

Ключові слова: *фазовий спектр, маскування інформації, канал передачі даних, пропускна здатність.*

Вступ

Постановка проблеми. Ефективне функціонування сучасних систем озброєння та військової техніки неможливе без відповідного інформаційного забезпечення. В першу чергу це обумовлено необхідністю швидкого обміну оперативною інформацією для прийняття рішень [1].

Аналіз останніх досліджень і публікацій. Аналіз основних тенденцій розвитку озброєння та військової техніки передових у військово-технічному відношенні держав, а також досвід збройних конфліктів останнього часу показує, що одним з пріоритетних напрямків в забезпеченні ефективного управління військами і силами є удосконалення засобів зв’язку та передачі даних [2].

На сьогоднішній день Збройні Сили України перебувають на етапі стрімкого розвитку з метою приведення усіх компонентів, у тому числі систем управління та обміну інформацією, до сучасного рівня. Найактуальнішими питаннями щодо інформаційного забезпечення, обміну та захисту інформації є впровадження наступних компонентів:

– сучасних технологій обміну оперативною інформацією;

– систем захисту інформації від несанкціонованого доступу;

– нових методів та алгоритмів обробки інформації;

– систем моніторингу та оцінки;

– інтелектуальних технологій прийняття рішень на основі штучного інтелекту [3].

В свою чергу досвід ведення бойових дій авіацією Повітряних Сил ЗС України під час проведення антитерористичної операції виявив проблемні недоліки існуючої системи інформаційної підтримки. Так, для успішного виконання бойового завдання екіпаж повітряного судна повинен бути своєчасно та достовірно забезпечений наступною інформацією, яка включає навігаційну інформацію та дані про район застосування авіаційних засобів ураження; інформацію про ціль, інформацію про засоби ППО противника, інформацію про літаки у складі групи, метеообстановку і т.д. [4]. Своєчасний та достовірний обмін визначеною інформацією вимагає використання сучасної каналоутворюючої апаратури з достатньою пропускною здатністю.

Обмін даними при забезпеченні інформаційної підтримки виконання завдань повітряними суднами забезпечується за рахунок використання частотної телеграфії в аналогових радіостанціях. Обмін інформацією відбувається при наявності блоку частотної телеграфії, який перетворює вхідну інформацію на сигнал звукового діапазону з двома частотами. При цьому логічному нулю відповідає значення низької

частоти, а логічній одиниці відповідає значення високої частоти.

У порівняні з аналоговими радіостанціями бортові засоби передачі інформації у цифровому вигляді мають переваги. Прикладом бортових цифрових засобів є багатофункціональна УКХ радіостанція RF-7850A-MR "Харріс" виробництва Сполучених Штатів Америки, яка забезпечує обмін повідомленнями відповідно до загальноприйнятих протоколів передачі даних (ASK DTE Data, ECCM IP Data, WBFSK/TCM DTE Data, WBFSK/TCM IP Data, ANW2Ce IP Data). При цьому можливо використання криптографічних алгоритмів забезпечення гарантованої захищеності повідомлень AES 256 та AES 126. В цілому радіостанція RF-7850A-MR забезпечує потреби щодо пропускної здатності каналів передачі інформацією для літаків Повітряних Сил Збройних Сил України. Але з іншого боку модернізація літаків на основі розглянутої радіостанції вимагає значних матеріальних затрат та впровадження стандартів НАТО.

Таким чином, у випадку впровадження технології обміну інформацією між літаками ПС ЗСУ при роботі у рамках єдиного інформаційного простору виникають обмеження, які представлено на рис. 1.

Рис. 1. Недоліки роботи обладнання

Іншим важливим аспектом функціонування систем обміну даними в умовах активного протистояння є забезпечення заданого рівня захищеності. Враховуючи досвід проведення АТО та ООС можна виділити наступні фактори, які впливають на загрозу інформаційної безпеки обміну даними:

1. Відсутність механізмів гарантованого забезпечення конфіденційності обміну даними авіації ПС ЗСУ.

2. Наявність на території протистояння підрозділів радіо та радіотехнічної розвідки країни-агресора.

3. Цінність та значимість інформації в умовах конфлікту.

4. Можливість знищення каналу передачі даних [5].

Можливим напрямком усунення виявлених обмежень при створенні каналів передачі даних з достатньою пропускною здатністю одночасно з забезпечення захищеності інформації є використання маскування інформації в мовних повідомленнях [6]. В цьому випадку маскування дозволяє приховати інформаційні повідомлення в контейнери не привертаючи уваги [7].

Мета статті – розробка методу прихованої передачі даних на основі маскування інформації в мовних повідомленнях.

Виклад основного матеріалу

Для задовільнення вимог, щодо забезпечення захисту інформації сформульовано наступні вимоги щодо методу маскування даних [8]:

1. Вимоги мінімізації спотворень голосового контейнера А.

Дана вимога характеризується тим, що величина $\eta(A; A')$, яка показує ступінь відмінності вихідного голосового контейнера A від перетвореного повідомлення A' повинна приймати мінімальне значення, а саме:

$$\eta(A; A') \to \min .$$

В цьому випадку буде забезпечуватись приховування інформаційного повідомлення одночасно з забезпеченням заданої якості мовних повідомлень.

2. Вимоги щодо незмінності інформаційного повідомлення B. Для оцінки ступеня схожості вихідного інформаційного повідомлення B відносно повідомлення B' після вилучення з контейнеру вводиться величина $\rho(B; B')$, яка характеризує метод з позиції спотворень, які вносяться в результаті передачі. У цьому випадку для забезпечення мінімальної відмінності між повідомленням B та B' величина $\rho(B; B')$ повинна приймати мінімальне значення.

3. Ймовірність $P_в$ виявлення противником наявності додаткової інформації в голосовому повідомленні повинна бути мінімальною. Ймовірність характеризує метод маскування інформації в мовних повідомленнях з позиції атаки на виявлення вбудовування.

4. Пропускна здатність Q прихованого каналу передачі інформації повинна бути максимальною:

$$Q \to \max .$$

5. Час $t_{маск}$ вбудовування інформації в голосове повідомлення повинно бути мінімальним:

$$t_{маск} \to \min .$$

Метод прихованої передачі інформації передбачає виконання маскування та демаскування інформаційного повідомлення.

Для розробки методу маскування розглянемо вихідне мовне повідомлення A (рис. 2), яке в подальшому необхідно розділити на фрагменти A_γ для маскування інформаційних повідомлень.

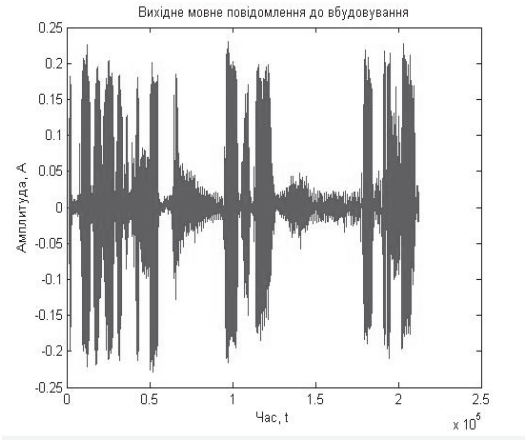

Рис. 2. Вихідне мовне повідомлення

Кількість фрагментів для голосового повідомлення А дорівнює G, яке обчислюється на основі наступного виразу:

$$G = \frac{T}{t},$$

де T – довжина голосового повідомлення А, с;

t – довжина фрагмента A_γ, с.

Голосове повідомлення підлягає дискретизації. При цьому необхідно забезпечити виконання критерію Найквіста-Шенона [9]. Враховуючи, що максимальне значення частоти $f_{\max}$ фрагменту голосового повідомлення A_γ дорівнює 20 кГц, розрахуємо значення частоти дискретизації f_∂ та часовий інтервал між дискретами Δt:

$$f_Д = 2 \cdot f_{\max} = 40 \text{ (кГц)},$$

$$\Delta t = \frac{1}{2 \cdot f_{\max}} = 0,000025 = 2,5 \cdot 10^{-5} \text{ (с)}.$$

Операція дискретизації задається наступним виразом:

$$I_\gamma = \varphi_Д(A_\gamma),$$

де I_γ – дискретизоване представлення фрагменту голосового повідомлення A_γ, $\gamma = \overline{1, G}$;

$\varphi_Д$ – функціонал, який описує операцію дискретизації.

Після операції дискретизації фрагмент голосового повідомлення I_γ буде мати наступний вигляд:

$$I_\gamma = \{i_1; i_2; ...; i_i; ...; i_N\}.$$

Тут i_i - i-та складова фрагмента I_γ голосового повідомлення, $i = \overline{1, N}$. Для розрахунку кількості складових для фрагменту після дискретизації використовується наступна формула:

$$N = \frac{t}{\Delta t}.$$

Наступний етап обробки фрагменту передбачає виконання фільтрації. Враховуючи, що в існуючих аналогових засобах радіозв'язку голосові повідомлення підлягають фільтрації з метою виділення сигналу на частотах мовних повідомлень від $f_{c\min} = 300$ Гц до $f_{c\max} = 3400$ Гц, то в процесі передачі повідомлень можливо знищення частини інформації, яка передається. Звідси, необхідно провести попередню обробку шляхом цифрової фільтрації фрагмента I_γ.

Значить необхідно отримати спектр голосового повідомлення на основі використаня дискретного перетворення Фур'є за допомогою формули:

$$y_k = \sum_{i=1}^{N} i_i \cdot e^{\frac{i2\Pi}{N} ki},$$

де y_k –комплексна амплітуда, яка відповідає значенню сигналу на частоті k, $k = \overline{1, K}$.

i_i - i –та складова фрагмента I_γ голосового повідомлення, $i = \overline{1, N}$. Враховуючи, що ДПФ може виконуватись для різного значення $K = \overline{1,20000}$ компонент розкладу сигналу, то для відповідності позиції спектральної компоненти реальному значенню частоти сигналу необхідно виконати наступний розрахунок:

$$k_c = \frac{K \cdot f_c}{20000}.$$

Тут K – кількість компонент спектрального розкладу ДПФ; f_c – необхідне значення частоти сигналу; k_c – компонента спектрального представлення, яка відповідає частоті f_c. Спектральне представлення Y_γ фрагменту I_γ голосового повідомлення буде мати вигляд:

$$Y_\gamma = \{y_1; y_2; ...; y_k; ...; y_K\}.$$

Тоді операція цифрової фільтрації буде виконуватись на основі системи рівнянь:

$$y_k^{'} = \begin{cases} y_k \cdot \lambda, \to k = 1...k_{c\min} \ \& \ \lambda = 0; \\ y_k \cdot \lambda, \to k = k_{c\min}...k_{c\max} \ \& \ \lambda = 1; \\ y_k \cdot \lambda, \to k = k_{c\max}...f_{\max} \ \& \ \lambda = 0. \end{cases}$$

Тут $y_k^{'}$ - k-та спектральна компонента голосового фрагменту I_γ після операції фільтрації;

λ – коефіцієнт фільтрації.

Для забезпечення виконання вимог до розробленого методу щодо зменшення спотворень вихідного повідомлення пропонується вбудовування інформаційного повідомлення виконувати шляхом модифікації фази. На відміну від амплітуди та частоти мовного повідомлення, фаза звукового сигналу не містить семантичної інформації та її модифікація не впливатиме на слухове сприйняття людиною. Іншими словами фаза мовного повідомлення уявляє

собою надлишковість. Звідси пропонується використовувати таку надлишковість для вбудовування інформації. Для виділення фазових складових $\{\varphi_k\}$ фрагменту мовного повідомлення I_γ зі значення частотного спектру Y_γ після фільтрації використовується наступний вираз:

$$\varphi_k = arctg\,(\,y_k^{(I)} - y_k^{(R)})\,,$$

де $y_k^{(I)}$ – k-та компонента уявної частини спектральної складової y_k, $k = \overline{1, K}$;

$y_k^{(R)}$ – k-та компонента реальної частини спектральної складової y_k, $k = \overline{1, K}$.

У цьому випадку отримаємо фазовий спектр Φ_γ, який буде мати вигляд:

$$\Phi_\gamma = \{\varphi_1, \varphi_2, ..., \varphi_k, ..., \varphi_K\},$$

де φ_k – k-та компонента фазового спектру, $k = \overline{1, K}$.

На наступному етапі відбувається вбудовування бітів інформаційного повідомлення шляхом модифікації складових фазового спектру *B*. У роботі пропонується алгоритм прихованого вбудовування даних шляхом зміни значення фази мовного повідомлення на заздалегідь фіксовані значення. Але в цьому випадку існує можливість виявлення модифікації при аналізі фазового спектру повідомлення. Тому пропонується здійснювати непряму модифікацію значень фаз однієї складової відносно наступної складової у фрагменті мовного повідомлення [10].

Приховане вбудовування даних здійснюється у двійковому вигляді, таким чином щоб елемент b повідомлення B, яке приймає наступний вигляд $b = [0; 1]$. Здійснюється поділ фазового спектру Φ_γ на пари складових φ_1 та φ_2 та їх модифікація за правилом:

– якщо біт інформаційного повідомлення приймає значення $b = 1$, то виконується умова $\varphi_1 > \varphi_2$;

– і навпаки, якщо біт інформаційного повідомлення приймає значення $b = 0$, то виконується умова $\varphi_1 < \varphi_2$. Для операції модифікації використовується наступна формула:

$$\varphi_{\text{mod}} = \left(\frac{|\varphi_2|}{|\varphi_1|}\right) \cdot \varphi \cdot k_{\text{mod}},$$

де k_{mod} – коефіцієнт модифікації, який характеризує ступінь зміни модифікованої фази φ_{mod} відносно вихідної φ.

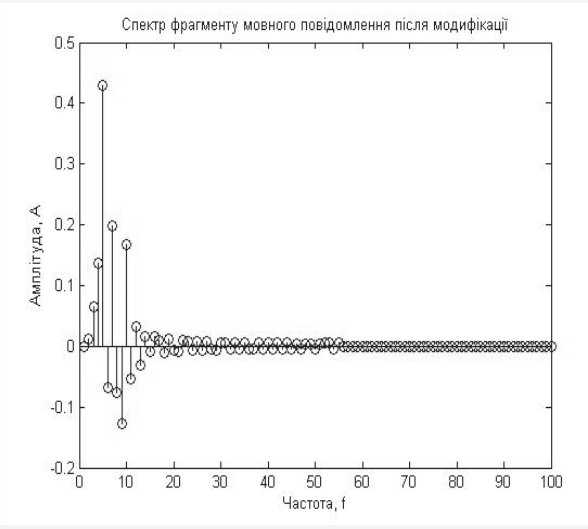

Рис. 3. Фазовий спектр фрагменту мовного повідомлення після модифікації

На основі модифікованої фази здійснюється перехід до частотного спектру за допомогою формули:

$$y_k'' = (\sqrt{(y_k^{(I)} - y_k^{(R)})}) \cdot e^{(-j) f_{mod}}.$$

На наступному етапі пропонується застосувати формулу зворотного дискретного перетворення Фур'є:

$$i_i = \frac{1}{N} \sum_{k=1}^{I} y_k \cdot e^{\frac{i2\Pi}{N} ki}.$$

Після чого отримуємо сигнал (в часовій області), в якому буде міститися модифікована інформація (рис. 4).

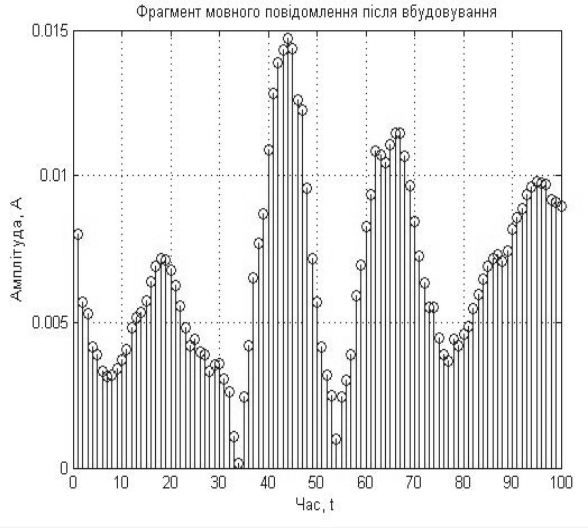

Рис. 4. Фрагмент мовного повідомлення після вбудовування

Схема роботи алгоритму маскування інформаційного повідомлення представлена на рис. 5.

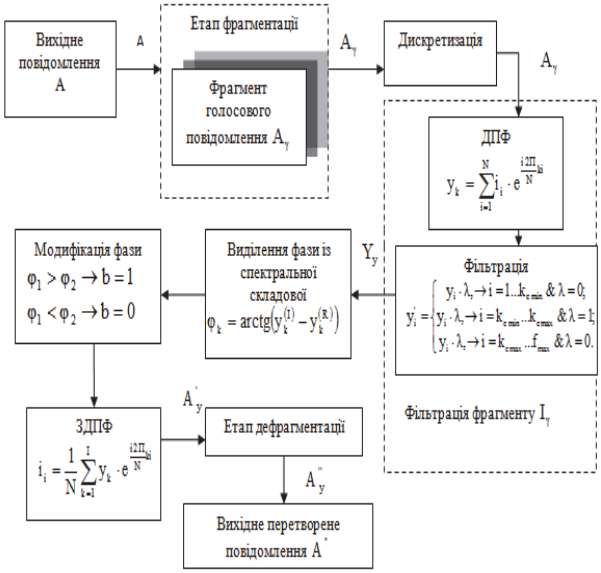

Рис. 5. Схема прямого маскування мовного повідомлення

Остаточна композиція модифікованого голосового повідомлення відбувається на основі сумування всіх фрагментів (рис. 6).

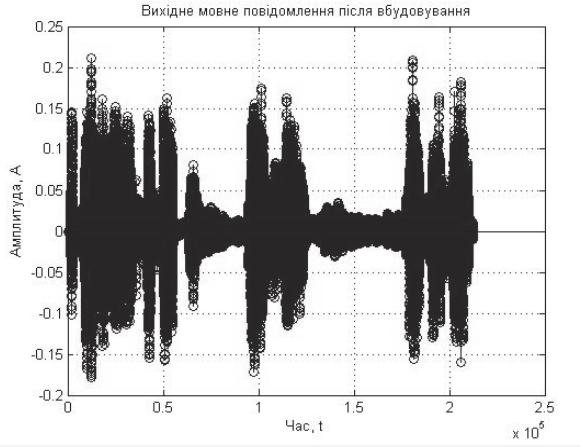

Рис. 6. Модифіковане мовне повідомлення після вбудовування

Отримане повідомлення подається на вхід до аналогової каналоутворюючої апаратури.

Метод демаскування передбачає відновлення вихідного мовного повідомлення. Схема демаскування мовного повідомлення наведена на рис. 7 та відбувається у зворотному напрямку від маскування.

Процес вилучення замаскованого повідомлення буде включати в себе наступні етапи:

1. Нехай $A^{"}$ – отримане мовне повідомлення, яке розбивається на фрагменти $A^{"}_{\gamma}$. Кількість фрагментів для голосового повідомлення $A^{"}_{\gamma}$ дорівнює G, яке обчислюється на основі наступного виразу:

$$G = \frac{T}{t},$$

де T – довжина голосового повідомлення $A^{"}$, секунд; t – довжина фрагмента $A^{"}_{\gamma}$, с.

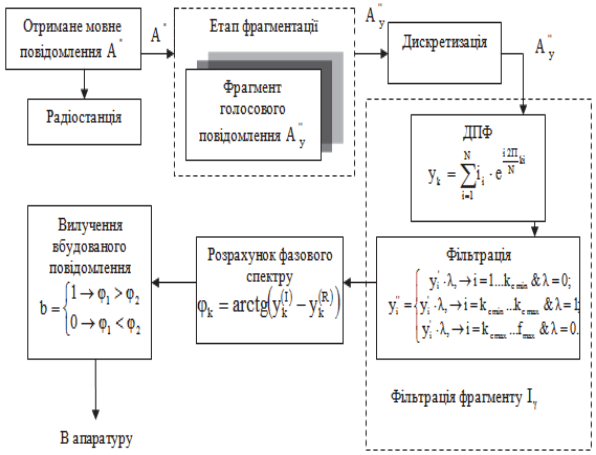

Рис. 7. Схема демаскування мовного повідомлення

2. Голосове повідомлення підлягає дискретизації. Операція дискретизації задається наступним виразом:

$$I_\gamma = \varphi_Д(A^{"}_{\gamma}),$$

де I_γ – фрагмент голосового повідомлення $A^{"}_{\gamma}$, $\gamma = \overline{1, G}$; $\varphi_Д$ – функціонал, який описує операцію дискретизації.

3. Наступний етап обробки фрагменту передбачає виконання цифрової фільтрації фрагмента I_γ.

Значить необхідно отримати спектр голосового повідомлення дискретного перетворення Фур'є за допомогою формули:

$$y_k = \sum_{i=1}^{N} i_i \cdot e^{\frac{i2\Pi}{N}ki},$$

де y_k – комплексна амплітуда, яка відповідає значенню сигналу на частоті k, $k = \overline{1, K}$;

i_i - i-та складова фрагмента I_γ голосового повідомлення, $i = \overline{1, N}$.

Операція цифрової фільтрації буде виконуватись на основі системи рівнянь:

$$y^{"}_k = \begin{cases} y^{'}_k \cdot \lambda, \rightarrow k = 1.....k_{c\min} \ \& \ \lambda = 0; \\ y^{'}_k \cdot \lambda, \rightarrow k = k_{c\min}...k_{c\max} \ \& \ \lambda = 1; \\ y^{'}_k \cdot \lambda, \rightarrow k = k_{c\max}....f_{\max} \ \& \ \lambda = 0. \end{cases}$$

Тут $y^{"}_k$ - k-та спектральна компонента голосового фрагменту I_γ після операції фільтрації; λ - коефіцієнт фільтрації.

4. На даному етапі необхідно виділити фазу із спектральної складової. Розрахунок фазового спектру буде мати наступний вигляд:

$$\varphi_k^{"} = arctg\,(y_k^{'(I)} - y_k^{'(R)}),$$

де $y'^{(I)}_k$ – *k*-та компонента уявної частини спектру;

$y'^{(R)}_k$ – *k*-та компонента реальної частини спектру.

5. На наступному етапі здійснюється вилучення вбудованого повідомлення шляхом порівняння значень пар фаз за допомогою формули:

$$b = \begin{cases} 1 & \rightarrow \quad \varphi_1 > \varphi_2; \\ 0 & \rightarrow \quad \varphi_1 < \varphi_2. \end{cases}$$

Вилучене інформаційне повідомлення у двійковому вигляді може використовуватись обладнанням повітряного судна для забезпечення інформаційної підтримки бойового завдання [11]. Оцінка ефективності розробленого методу маскування інформаційних повідомлень відбувається на основі програмної моделі. Проводиться розрахунок пропускної здатності каналу у різних умовах модифікації мовних повідомлень [12]. На рис. 8 у графічному вигляді наведені значення пропускної здатності Q відносно пікового відношення сигнал/шум PSNR.

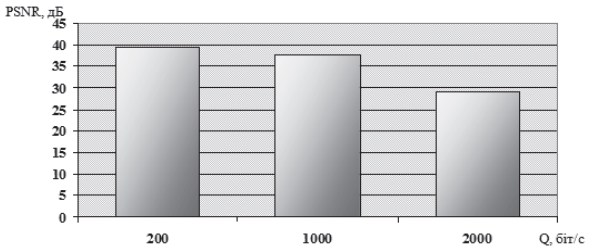

Рис. 8. Залежність значень пікового відношення сигнал/шум відносно пропускної здатності

З аналізу значень на рис. 8 можна зробити висновок , що найбільше значення пікового відношення сигнал/шум спостерігається для випадку, коли пропускна здатність мовного повідомлення дорівнює Q = 200 біт/с.

Висновки

В статті розроблено метод прихованої передачі інформації в мовному повідомленні на основі модифікації компонент фазового спектру за умовним правилом. Відмінною рисою методу є можливість приховати сам факт наявності вбудованого повідомлення.

Одночасно з реалізацією конфіденційності повідомлень, метод маскування додатково враховує питання забезпечення цілісності та доступності інформації.

Сформовано вимоги до методу, які полягають у мінімізації спотворень вихідного мовного повідомлення в результаті вбудовування інформації.

Проведено аналіз ефективності методу за величиною спотворень, які вносяться у вихідне повідомлення в процесі роботи алгоритму маскування.

Перспективним напрямком подальших досліджень є практична реалізація розробленого методу, тобто створення прихованого каналу передачі даних на основі існуючого обладнання для потреб бортових системи повітряного судна.

Список літератури

1. Радковець Ю.І. Погляди на створення системи інформаційної безпеки України та її Збройних Сил / Ю.І. Радковець, О.В. Левченко, О.М. Косогов // Наука і оборона. – 2014. – № 1. – С. 38-41.

2. Кірсанов С.О. Перспективи розвитку системи управління Збройних Сил України з використанням принципу єдиного інформаційного простору / С.О. Кірсанов // Наука і техніка Повітряних Сил Збройних Сил України. – 2010. – № 1(3). – С. 15-20.

3. Широчин С.С. Методи комбінованого стеганографічного захисту мультимедійних даних в хмарних сховищах: автореф. дис., канд. тех. наук: 05.13.05 / Широчин Семен Станіславови. – К.: Нац. тех. ун-т., 2015. – 16 с.

4. Кириченко І.О. Визначення поняття "інформаційно-бойовий простір", змісту та ролі його складових елементів для досягнення перемоги у воєнних конфліктах XXI століття / І.О. Кириченко, С.П. Ярош // Системи озброєння і військова техніка. – 2011. – № 3(27). – С. 102-108.

5. Довідник учасника АТО: озброєння і військова техніка Збройних Сил Російської Федерації / за заг. ред. А.М. Алімпієва. – Х.: Оригінал, 2015. – 732 с.

6. Метод хаотичного маскування фазоманіпульованих сигналів / П.Ю. Костенко, О.М. Чекунова, Н.М. Сидор, О.В. Моргун // Наука і техніка Повітряних Сил Збройних Сил України. – 2019. – № 1(34). – С. 84-90.

7. Максимова Л.П. Захист інформації / Л.П. Максимова. – К.: ВД "Інформатика", 2018. – 120 с.

8. Бекіров А.Е. Метод захисту інформації на основі стеганографічних систем / А.Е. Бекіров // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – № 1(18). – С. 130-133.

9. Кобозєва А.А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, В.О. Хорошко. – К.: Вид. ФОП Москаленко О.М., 2010. – 55 с.

10. Михайлов А.Н. Исследование анализа стойкости стеганографических алгоритмов / А.Н. Михайлов, З.Б. Холодная // Системи обробки інформації. – 2006. – № 6(55). – С. 130-135.

11. Обод І.І. Захист інформації в мережі систем спостереження повітряного простору / І.І. Обод, О.О. Стрельницький // Системи обробки інформації. – 2016. – № 2(139). – С. 47-49.

12. Франчук В.М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних / В.М. Франчук. – К.: НПУ, 2012. – 35 с.

References

1. Radkovets, Y.I., Levchenko, O.M. and Kosohov, O.M. (2014), "Poglyadi na stvorennya sistemi informacijnoї bezpeki Ukraini ta yiyi Zbrojnih Sil" [Views on the creation of the information security system of Ukraine and its Armed Forces], *Science and Defense*, No. 1, pp. 38-41.

2. Kirsanov, S.O. (2010), "Perspektivi rozvitku sistemi upravlinnya Zbrojnih Sil Ukraïni z vikoristannyam principu єdinogo informacijnogo prostoru" [Prospects for the development of the management system of the Armed Forces of Ukraine using the principle of a single information space], *Science and Technology of the Air Force of Ukraine*, No. 1(3), pp. 15-20.

3. Shyrochyn, S.S. (2015), "*Metodi kombinovanogo steganografichnogo zahistu mul'timedijnih danih v hmarnih skhovishchah*" [*Methods of combined steganographic protection of multimedia data in cloud storage*], Kyiv, 16 p.

4. Kyrychenko, I.O. and Yarosh, S.P. (2011), "Viznachennya ponyattya "informacijno-bojovij prostir", zmistu ta roli jogo skladovih elementiv dlya dosyagnennya peremogi u voyennih konfliktah XXI stolittya" [Definition of the concept "Information and combat space", the content and role of its constituent elements to achieve victory in the military conflicts of the XXI century], *Systems of Arms and Military Equipment*, No. 3(27), pp. 102-108.

5. Alimpiiev, A. (2015), "*Dovidnik uchasnika ATO: ozbroyennya i vijs'kova tekhnika Zbrojnih Sil Rosijs'koyi Federaciyi*" [*Reference book of the ATO Armed Forces and Military Equipment of the Armed Forces of the Russian Federation*], Original, Kharkiv, 732 p.

6. Kostenko, P.Y., Chekunova, O.M., Sydor, N.M. and Morhun, O.V. (2019), "Metod haotichnogo maskuvannya fazomanipul'ovanih signaliv" [Method of chaotic cutting of phasomanipulated signals], *Science and Technology of the Air Force of Ukraine*, No. 1(34), pp. 84-90.

7. Maksimova, L. (2018), "*Zahist informacii*" [*Information protection*], KNU, Kyiv, 120 p.

8. Bekirov, A.E. (2015), "Metod zahistu informacii na osnovi steganografichnih sistem" [Method of protection informations on the basis of steganographic systems], *Science and Technology of the Air Force of Ukraine*, No. 1(18), pp. 130-133.

9. Kobozieva, A. and Khoroshko, V. (2010), "*Analiz zahishchenosti informacijnih sistem*" [*Analysis of the security of information systems*], FOP Moskalenko O.M., Kyiv, 155 p.

10. Mikhailov, A.N. and Kholodnaia, Z.B. (2006), "Issledovanie analiza stojkosti steganograficheskih algoritmov" [The study of the analysis of the resistance of steganographic algorithms], *Information Processing Systems*, No. 6(55), pp. 130-135.

11. Obod, A.A. and Strelnytskyi, A.A. (2016), "Zahist informacii v merezhi sistem sposterezhennya povitryanogo prostoru" [Data protection in the network of observation airspace], *Information Processing Systems*, No. 2(139), pp. 47-49.

12. Franchuk, V. (2012), "*Zahist informacijnih resursiv: kriptografichni ta steganografichni metodi zahistu danih*" [*Information resources protection: cryptographic and steganographic data protection methods*], NPU, Kyiv, 235 p.

Надійшла до редколегії 18.02.2019
Схвалена до друку 23.04.2019

Відомості про авторів:

Бекіров Алі Енверович
кандидат технічних наук викладач
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-6155-0597

Баранік Олексій Миколайович
кандидат технічних наук старший викладач
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-1499-7943

Парфило Вікторія Вікторівна
курсант Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-4938-0978

Information about the authors:

Ali Bekirov
Candidate of Technical Science
Lecturer of Ivan Kozhedub Kharkiv National
Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-6155-0597

Oleksii Baranik
Candidate of Technical Science Senior Instructor
of Ivan Kozhedub Kharkiv National
Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-1499-7943

Viktoriia Parfylo
Cadet of Ivan Kozhedub Kharkiv National
Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-4938-0978

МЕТОД СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ В ГОЛОСОВОМ СООБЩЕНИИ

А.Е. Бекиров, А.Н. Бараник, В.В. Парфило

В статье рассматривается актуальный вопрос функционирования системы информационной поддержки выполнения боевых заданий экипажами воздушных суден. Анализируются образцы существующего отечественного и заграничного оборудования обмена информационными сообщениями. Для устранения выявленных ограничений относительно функционирования рассмотренного оборудования в едином информационном пространстве предлагается направление, которое предусматривает маскировку данных в голосовых сообщениях с дальнейшей передачей в аналоговых радиостанциях. Сформированы требования к алгоритму, которые заключаются в минимизации искажений исходящего голосового сообщения в результате встраивания информации. Разработан метод маскировки данных в голосовых сообщениях на основе модификации фаз фрагментов по непрямому правилу. На основе программной модели проведена оценка разработанного метода.

***Ключевые слова**: фазовый спектр, маскирование информации, канал передачи данных, пропускная способность.*

METHOD OF HIDDEN TRANSFER OF INFORMATION IN VOICE MESSAGE

A. Bekirov, O. Baranik, V. Parfylo

The article deals with the actual question of the functioning of the information support system for the performance of combat missions by aircraft crews. Samples of existing domestic and foreign equipment for the exchange of information messages are analyzed. On the basis of the analysis, it was discovered that the existing radio station of the domestic specimen does not meet modern requirements for the protection of information. At the same time, the RF-7850A-MR provides the bandwidth requirements of the data channels and the level of security. But the modernization of aircraft on the basis of the considered radio station requires significant material costs and implementation of NATO standards. The factors influencing the threat of information security of data exchange, taking into account the experience of ATO and EOS, were also analyzed. An important aspect of the operation of data exchange systems in conditions of active confrontation is to provide a given level of security. In order to eliminate the revealed restrictions on the functioning of the considered equipment in a single information space, a direction is proposed that provides for the masking of data in voice messages with further transmission in analogue radio stations. The requirements for the algorithm are formed, which consist in minimizing the distortion of the outgoing voice message as a result of embedding information. A method for masking data in voice messages based on modifying the phases of fragments according to an indirect rule has been developed. In this case, masking allows you to hide the information messages in the containers without attracting attention. An algorithm for disguising information from a speech message is also developed, the binary information extracted can be used by aircraft equipment to provide information support for combat missions. Based on the software model, the developed method was assessed.

***Keywords:** phase spectrum, information masking, data channel, throughput.*