Зв'язок, радіотехніка, радіолокація, акустика та навігація

УДК 681.324 DOI: 10.30748/zhups.2020.65.10

В.В. Парфило, А.Е. Бекіров, В.В. Парфило, С.А. Ковтуненко

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

МЕТОД ЗАВАДОСТІЙКОГО КОДУВАННЯ МОВНОГО ПОВІДОМЛЕННЯ З ПРИХОВАНИМ ВБУДОВУВАННЯМ ДОДАТКОВОЇ ІНФОРМАЦІЇ

У статті розглядається актуальне питання підвищення рівня інформаційної захищеності авіації Повітряних Сил Збройних Сил України на основі використання методу завадостійкого кодування. Проводиться аналіз штатного обладнання обміну даними та існуючих методів кодування мовного повідомлення, формулюються основні недоліки. Для усунення виявлених недоліків пропонується використання завадостійкого коду Хеммінга, який передбачає виявлення та виправлення помилок, які виникли під час передачі мовного повідомлення. На основі кодування Хеммінга розроблений метод для приховування додаткової інформації в мовному повідомленні. Створено систему прямого та зворотного кодування на основі розробленого методу.

Ключові слова: *кодування Хеммінга, приховане вбудовування даних, канал передачі даних, біт.*

Вступ

Постановка проблеми. На сьогоднішній день ефективність функціонування Збройних Сил України напряму залежить від організованого, якісного, завадозахищеного зв'язку. Особливої важливості дане питання набуває під час виконання завдань в умовах проведення Операції Об'єднаних Сил. В першу чергу це обумовлено необхідністю приведення існуючих бортових засобів зв'язку до сучасних вимог та стандартів [1].

Аналіз останніх досліджень і публікацій. Аналіз основних напрямків розвитку військової техніки противника, а також досвіду локальних війн, конфліктів та навчань свідчить про те, що удосконалення засобів зв'язку та передачі даних у ході проведення Операції Об'єднаних Сил стають однією із головних умов для успішного виконання бойового завдання.

Для сучасних країн характерною рисою є функціонування різних елементів Збройних Сил у єдиному інформаційному просторі (рис. 1) [2].

Рис. 1. Схема взаємодії компонентів Збройних Сил у єдиному інформаційному просторі

Джерело: розроблено авторами за даними [1, С. 74].

Таке функціонування потребує відповідного удосконалення засобів зв'язку і передачі даних, всіх видів інформаційного забезпечення і автоматизації управління.

При створені каналів передачі даних актуальним питанням є підвищення рівня інформаційної захищеності, що в свою чергу впливає на своєчасний та якісний обмін інформаційними повідомленнями. Але в умовах збройного протистояння для каналу передачі даних існують загрози порушення складових інформаційної безпеки, такі як:

– загрози доступності інформаційних повідомлень;

– загрози цілісності;

– загрози конфіденційності обміну даними.

Значить, для забезпечення обміну повідомленнями між повітряними суднами при роботі в єдиному інформаційному просторі в умовах складної радіотехнічної обстановки необхідно одночасно з розробкою методу прихованої передачі інформації забезпечити інформаційну захищеність даних [3].

Серед сучасних засобів забезпечення обміну інформацією є аналогові радіостанції, які при роботі в єдиному інформаційному просторі мають системні недоліки. Основними недоліками є недостатня пропускна здатність та відсутність інформаційної захищеності обміну даними [4].

Бортові засоби обміну даними у цифровому вигляді мають велику перевагу над аналоговими радіостанціями.

Прикладом бортових цифрових засобів є багатофункціональна УКХ-радіостанція 9681 V/UHF ви-

робництва компанії Aselsan (Туреччина). Це сучасна цифрова завадозахищена багатодіапазонна радіостанція, яка дозволяє взаємодіяти з відповідними наземними та морськими засобами. Дана радіостанція встановлена на ЛА Збройних Сил Турецької Республіки та деяких інших країн. Радіостанція працює в таких режимах: передача даних на фіксованих частотах з забезпеченням псевдовипадкової перебудови робочої частоти (ППРЧ); відкрита передача інформації (голосової та параметричної); закрита передача даних (з криптографічним захистом). Найбільш актуальним на даний час як в авіації, так і в інших військах (силах) Збройних Сил України є завдання щодо впровадження цифрових завадозахищених радіостанцій. Але модернізація літаків на основі розглянутої радіостанції вимагає значних матеріальних затрат та впровадження стандартів НАТО [5].

Проведено аналіз існуючого методу прихованої передачі інформації [6]. Даний метод полягає в тому, що приховані повідомлення кодуються всередині голосового повідомлення за допомогою контейнера таким чином, що змін не помітити і тільки одержувач повідомлення може розкодувати його.

На основі аналізу статті [6] встановлено, що розроблений метод має деякі недоліки, а саме:

– спотворення, які вносить дискретне перетворення Фур'є (ДПФ) при переході у частотну область;

– складність в обчисленні;

Для усунення виявлених недоліків пропонується розробити метод, який буде здійснювати приховану передачу даних в голосовому повідомленні без внесення в нього спотворень. Для цього пропонується:

– не застосовувати ДПФ, а здійснювати перетворення в просторово-часовій області;

– для забезпечення стійкості до активних впливів застосовувати завадостійке кодування [7].

Мета статті – розробка методу прихованої передачі даних в мовних повідомленнях на основі завадостійкого кодування.

Виклад основного матеріалу

Розглянемо вихідне мовне повідомлення A, яке розбивається на фрагменти A_γ.

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

$$G = \frac{T}{t}, \qquad (1)$$

де T – довжина голосового повідомлення A, секунд;

t – довжина фрагмента A_γ, секунд.

Голосове повідомлення підлягає дискретизації. При цьому необхідно забезпечити виконання критерію Найквіста-Шенона [8]. Враховуючи, що максимальне значення частоти $f_{\max}$ фрагменту голосового повідомлення A_γ дорівнює 20 кГц, розрахуємо мінімально необхідне значення частоти дискретизації f_∂ та часовий інтервал між дискретами Δt:

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

$$\Delta t = \frac{1}{2 \cdot f_{\max}} = 0,000025\,(c). \qquad (3)$$

Операція дискретизації задається наступним виразом:

$$I_\gamma = \varphi_Д(A_\gamma), \qquad (4)$$

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

f_∂ – функціонал, який описує операцію дискретизації.

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

$$I_\gamma = \{i_1; i_2; ...; i_i; ...; i_N\}, \qquad (5)$$

де 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:

$$N = \frac{t}{\Delta t}, \qquad (6)$$

де N – кількість елементів в одному фрагменті.

Наступний етап передбачає перетворення фрагменту мовного повідомлення у двійкову систему числення [9] за допомогою формули:

$$y_\gamma = f(I_\gamma), \qquad (7)$$

де $f(I_\gamma)$ – функціонал для переходу у двійкову область.

Тоді представлення у двійковій системі числення y_γ фрагменту I_γ голосового повідомлення буде мати наступний вигляд:

$$y_\gamma = \{y_1; y_2; ...; y_i; ...; y_N\}, \qquad (8)$$

де y_i – i-та складова фрагмента y_γ голосового повідомлення, $i = \overline{1,N}$.

У цьому випадку отримаємо бітову послідовність i-го елемента γ-го фрагмента, який буде мати вигляд:

$$y_1^{(\gamma)} = \{a_1; a_2; ...; a_1; ...; a_L\} \to a \in [0;1], \qquad (9)$$

де a_l – l-та компонента бітової послідовності, $l = \overline{1,L}$.

Для розрахунку кількості біт, які будуть міститися в $y_1^{(\gamma)}$-му елементі після переходу у двійкову

систему числення використовується наступна формула:

$$L = [\log_2 y] + 1. \quad (10)$$

Етапи перетворення мовного повідомлення зображені на рис. 2.

Для того, щоб забезпечити взаємооднозначність прямого та зворотного перетворення необхідно привести всі компоненти до одного значення. Іншими словами, необхідно щоб кількість біт на представлення одного компонента була рівною для всіх компонентів.

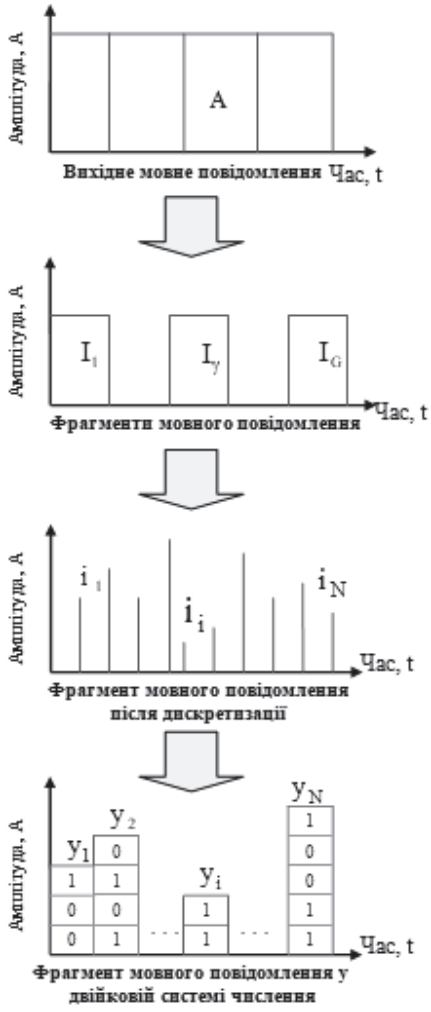

Рис. 2. Етапи перетворення мовного повідомлення
Джерело: розроблено авторами.

Для забезпечення даної рівності потрібно знайти елемент з максимальним значенням. Максимальне значення двійкового елементу знаходиться за формулою:

$$y^{\gamma}_{i_{\max}} = \max\{y^{\gamma}_i\}. \quad (11)$$

Враховуючи максимальне значення двійкового елементу $y^{\gamma}_{i_{\max}}$ розрахуємо кількість бітів, які будуть міститися в цьому елементі, використовуючи наступну формулу:

$$L_{\max} = [\log_2 y^{\gamma}_{i_{\max}}] + 1. \quad (12)$$

Значить для розрахунку кількості бітів Q_i, які необхідно додати до елементу y^{γ}_i, використовується наступний вираз:

$$Q_i = L_{\max} - L_i, \quad (13)$$

де L_i – кількість бітів i-го елементу γ-го фрагменту.

Тоді з урахуванням доданих біт $\{a_q\}$, i-й елемент γ-го фрагменту буде мати вигляд (рис. 3):

$$y^{\gamma}_i = \{a_1; a_2; ...; a_l; ...; a_L; a'_1; a'_2; ...; a'_q; ...; a'_Q\} = \\ = \{b_1; ...; b_l; ...; b_{L_{\max}}\}, \quad (14)$$

де $b_l - l$-та компонента бітової послідовності, $l = \overline{1, L_{\max}}$.

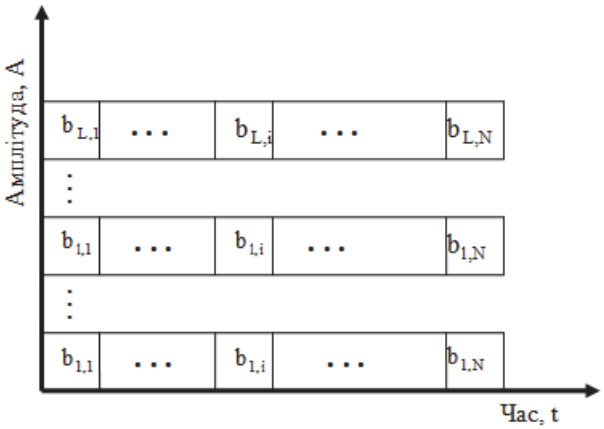

Рис. 3. Фрагмент мовного повідомлення
з урахуванням доданих бітів
Джерело: розроблено авторами.

На наступному етапі здійснюється формування кодового слова по рядках:

$$R_1 = \{b_{1,l}; ...; b_{1,i}; ...; b_{1,N}\} = \{r^{(1)}_1; ...; r^{(1)}_i; ...; r^{(1)}_N\} \\ \vdots \\ R_1 = \{b_{1,l}; ...; b_{1,i}; ...; b_{1,N}\} = \{r^{(l)}_1; ...; r^{(l)}_i; ...; r^{(l)}_N\} \quad (15) \\ \vdots \\ R_L = \{b_{L,1}; ...; b_{L,i}; ...; b_{L,N}\} = \{r^{(L)}_1; ...; r^{(L)}_i; ...; r^{(L)}_N\}.$$

Після чого здійснюється кодування Хеммінга по рядкам за допомогою формули (рис. 4):

$$R' = f(R_l), \quad (16)$$

де R' – послідовність бітів після застосування коду Хеммінга;

f – функціонал, який описує операцію кодування;

$R_l - l$-тий рядок бітової площини, $l = \overline{1; L_{\max}}$.

Довжина рядка Z не буде дорівнювати довжині вихідного рядка N, тому що кодування Хеммінга передбачає додаткові перевірочні біти. Тому розра-

хуємо довжину рядка бітової послідовності після застосування коду, використовуючи наступну формулу:

$$Z = N + \log_2[N] + 1, \quad (17)$$

де N – довжина рядка до застосування коду Хеммінга.

Тоді з урахуванням бітів, які додаються внаслідок застосування коду, рядок бітової послідовності буде мати вигляд:

$$R^{'} = \{r_1^{'}; ...; r_z^{'}; ...; r_Z^{'}\}. \quad (18)$$

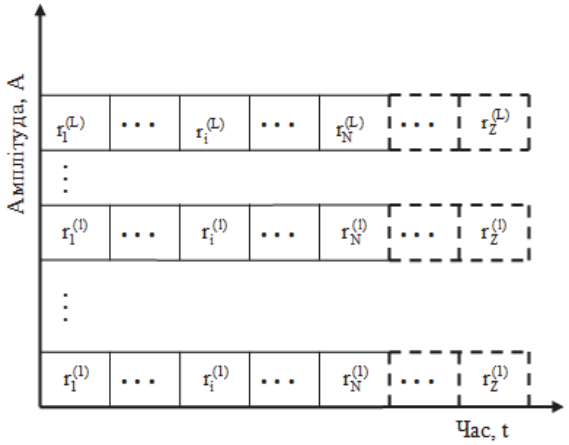

Рис. 4. Фрагмент мовного повідомлення після застосування коду Хеммінга
Джерело: розроблено авторами.

Наступний етап передбачає вибір позиції вбудовування інформації, яку потрібно приховати та опис її правила [10]. Даних правил існує безліч. Одним з таких правил є вбудовування інформаційних біт на будь-яку позицію. Тому правило позиції вбудовування можемо представити у вигляді:

$$\theta_{(1)} = (N - 1) + 1. \quad (19)$$

$$\theta_{(L_{\max})} = (N - L_{\max}) + 1, \quad (20)$$

де $\theta_{(l)}$ – позиція вбудовування, $\theta = \overline{1; N}$, $l = \overline{1; L_{\max}}$

Правило вбудовування задається наступним виразом (рис. 5):

$$r_{\theta}^{'} = \begin{cases} 0 & \rightarrow b_S = 0; \\ 1 & \rightarrow b_S = 1, \end{cases} \quad (21)$$

де $r_{\theta}^{'}$ – модифіковане значення біт в які вбудовується інформація;

b_S – значення модифікованого інформаційного біта.

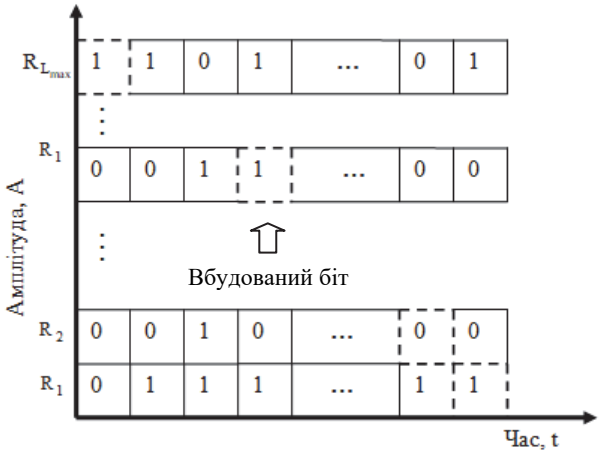

Рис. 5. Фрагмент мовного повідомлення після вбудовування інформаційних бітів за правилом
Джерело: розроблено авторами.

Отримане повідомлення готове для передачі до радіостанції. Схема роботи алгоритму представлена на рис. 6.

Метод декодування передбачає відновлення вихідного мовного повідомлення.

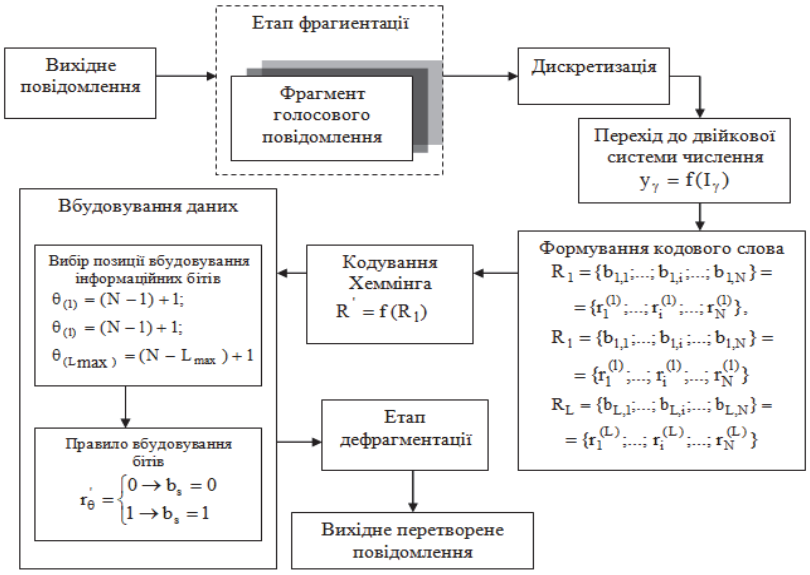

Рис. 6. Схема прямого перетворення мовного повідомлення
Джерело: розроблено авторами.

Процес вилучення вбудованого повідомлення буде включати в себе наступні етапи:

1. Припустимо що A'' – отримане мовне повідомлення, яке розбивається на фрагменти A''_γ. Кількість фрагментів для голосового повідомлення A'' дорівнює G, яке обчислюється на основі наступного виразу:

$$G=\frac{T}{t}, \tag{22}$$

де T – довжина голосового повідомлення A'', секунд;

t – довжина фрагмента A''_γ, секунд.

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

$$I_\gamma = \varphi_Д(A''_\gamma), \tag{23}$$

де I_γ – фрагмент голосового повідомлення A''_γ, $\gamma = \overline{1, G}$;

f_∂ – функціонал, який описує операцію дискретизації.

3. Наступний етап обробки фрагменту передбачає його перетворення у двійкову систему числення за допомогою формули:

$$y_\gamma = f(I_\gamma), \tag{24}$$

де $f(I_\gamma)$ – функціонал для переходу у двійкову область.

4. Необхідно знайти позиції інформаційних бітів. Правило позиції бітів буде мати наступний вигляд:

$$\theta_{(1)} = (N\text{-}1)+1. \tag{25}$$

$$\theta_{(l)} = (N\text{-}l)+1. \tag{26}$$

$$\theta_{(L_{\max})} = (N - L_{\max})+1, \tag{27}$$

де $\theta_{(l)}$ – позиція вбудовування, $\theta = \overline{1; N}$, $l = \overline{1; L_{\max}}$.

5. На наступному етапі здійснюється формування кодового слова за допомогою формули:

$$\begin{aligned} R_1 &= \{b_{1,l};...;b_{1,i};...;b_{1,N}\} = \{r_1^{(1)};...;r_i^{(1)};...;r_N^{(1)}\} \\ &\vdots \\ R_1 &= \{b_{1,l};...;b_{1,i};...;b_{1,N}\} = \{r_1^{(l)};...;r_i^{(l)};...;r_N^{(l)}\} \\ &\vdots \\ R_L &= \{b_{L,1};...;b_{L,i};...;b_{L,N}\} = \{r_1^{(L)};...;r_i^{(L)};...;r_N^{(L)}\}. \end{aligned} \tag{28}$$

6. Далі використовується декодування Хеммінга по рядкам за допомогою виразу:

$$R' = f^{-1}(R_l), \tag{29}$$

де R' – послідовність бітів після застосування зворотного коду Хеммінга,

R_l – l-тий рядок бітової площини, $l = \overline{1; L_{\max}}$.

Вилучене інформаційне повідомлення у двійковому вигляді може використовуватись обладнанням повітряного судна для забезпечення інформаційної підтримки бойового завдання [11].

Оцінка ефективності розробленого методу завадостійкого кодування мовного повідомлення проводиться на основі розрахунку кількості інформаційних біт $Q_{біт}$, які можуть бути вбудовані в голосове повідомлення тривалістю T [12].

Розрахуємо кількість елементів, які будуть міститися в мовному повідомленні N тривалістю T до застосування кодування Хеммінга, їх кількість обчислюється з урахуванням часового інтервалу між дискретами Δt:

$$N = \frac{T}{\Delta t}. \tag{30}$$

Враховуючи кількість елементів до кодування, обчислюється кількість елементів, які будуть міститися в мовному повідомленні після кодування Хеммінга Z:

$$Z = N + \log_2[N] + 1. \tag{31}$$

У якості приклада розрахуємо кількість інформаційних біт $Q_{біт}$ для голосового повідомлення довжиною $T = 1$ секунд з частотою $\Delta f = 22500\,Гц$.

Тоді кількість елементів, які будуть міститися в мовному повідомленні N обчислюються за формулою:

$$N = \frac{T}{\Delta t}. \tag{32}$$

Для даної формули необхідно розрахувати часовий інтервал між дискретами Δt, який розраховується за виразом:

$$\Delta t = \frac{1}{\Delta f} = 44\times10^{-6}\,(c). \tag{33}$$

На основі знайденого інтервалу між дискретами , розраховується кількість елементів N для мовного повідомлення:

$$N = \frac{T}{\Delta t} = \frac{1}{44\times10^{-6}} = 22501(біт). \tag{34}$$

Далі розрахуємо кількість елементів, які будуть міститися в мовному повідомленні після кодування Хеммінга Z:

$$\begin{aligned} Z = N + [\log_2 N] + 1 = 22501 + [\log_2 22501] + 1 = \\ = 22516(біт). \end{aligned} \tag{35}$$

Вбудовування інформаційних біт в елемент голосового повідомлення здійснюється після кодування Хеммінга, тому кількість вбудованих біт $Q_{біт}$ дорівнює кількості елементів Z:

$$Q_{біт} = Z = 22516(біт). \tag{36}$$

Отже, пропускна здатність P прихованого каналу передачі даних на основі розробленої технології забезпечується на рівні $P = 22516\,(біт/с)$.

Висновки

В статті розглянуто принцип функціонування різних елементів ЗС у єдиному інформаційному просторі.

Проведено аналіз штатного обладнання обміну даними та існуючих методів прихованої передачі інформації в мовному повідомленні.

На основі аналізу встановлено, що розглянутий метод має ряд системних обмежень. Для усунення виявлених недоліків було запропоновано на основі існуючого обладнання розробити метод завадостійкого кодування мовного повідомлення з прихованим вбудовуванням додаткової інформації.

Розроблений метод забезпечує виявлення та виправлення помилок, які виникають під час передачі мовного повідомлення і разом з тим приховування додаткової інформації в ньому.

Розроблено метод зворотного перетворення мовного повідомлення, який передбачає отримання вбудованої інформації на приймальній стороні.

Проведено аналіз ефективності методу на основі розрахунку кількості інформаційних біт, які можуть бути вбудовані в голосове повідомлення.

Напрямком подальшої роботи над методом є практична реалізація розробленого методу на основі існуючого бортового обладнання повітряного судна.

Список літератури

1. Кучеренко Ю.Ф. Основні шляхи розвитку систем управління військами та зброєю на сучасному етапі / Ю.Ф. Кучеренко, О.М. Гузько // Системи озброєння і військова техніка. – 2008. – № 4(16). – С. 73-76.

2. 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.

3. 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.

4. Організація військового зв'язку / В.Г. Шолудько, М.Ю. Єсаулов, О.В. Вакуленко, Т.Г. Гурський, М.М. Фомін. – К.: ВІТІ, 2017. – 282 с.

5. Гурський Т.Г. Аналіз шляхів вдосконалення засобів радіозв'язку мережі радіодоступу військової телекомунікаційної системи / Т.Г. Гурський // Збірник наукових праць Київського політехнічного інституту. – 2007. – № 1. – С. 30-40.

6. Бекіров А.Е. Метод прихованої передачі інформації в мовному повідомленні / А.Е. Бекіров, О.М. Баранік, В.В. Парфило // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2019. – № 2(60). – С. 75-82. https://doi.org/10.30748/zhups.2019.60.10.

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

8. Бекіров А.Е. Стеганографічний метод на основі безпосереднього та непрямого вбудовування даних для областей зображення з різною насиченістю / А.Е. Бекіров, В.Ж. Ященок, О.М. Крейдун // Сучасні інформаційні технології у сфері безпеки та оборони. – 2019. – № 1(34). – С. 115-120. https://doi.org/10.33099/2311-7249/2019-34-1-115-120.

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

10. Кушнір О.І. Аналіз методів завадостійкого кодування у цифрових системах зв'язку / О.І. Кушнір, О.І. Тимочко, О.В. Сєвєрінов // Системи обробки інформації. – 2007. – № 9(67). – С. 63-65.

11. Бекіров А.Е. Метод забезпечення конфіденційності радіопереговорів авіації / А.Е. Бекіров, А.О. Краснорученський, Н.М. Ковтуненко // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2019. – № 2(60). – С. 83-90. https://doi.org/10.30748/zhups.2019.60.11.

12. Конахович Г.Ф. Концепція побудови обладнання захищеного радіотелефонного зв'язку для авіаційних застосувань / Г.Ф. Конахович, В.В. Антонов, В.Є. Курушкін // Безпека інформації. – 2014. – № 3(20). – С. 224-230.

Надійшла до редколегії 05.06.2020
Схвалена до друку 14.07.2020

Відомості про авторів:

Парфило Василь Васильович
заступник начальника факультету
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0001-7127-5739

Information about the authors:

Vasyl Parfylo
Deputy Commander of the Faculty of
at Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0001-7127-5739

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

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

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

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

Ковтуненко Станіслав Андрійович
Начальник навчального курсу
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0003-1320-1891

Stanislav Kovtunenko
Company Commander
of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0003-1320-1891

МЕТОД ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ ГОЛОСОВОГО СООБЩЕНИЯ СО СКРЫТЫМ ВСТРАИВАНИЕМ ДОПОЛНИТЕЛЬНОЙ ИНФОРМАЦИИ

В.В. Парфило, А.Е. Бекиров, В.В. Парфило, С.А. Ковтуненко

В статье рассматривается актуальный вопрос обеспечения заданного уровня информационной безопасности авиации ВВС в условиях современного вооруженного противостояния. Рассмотрен принцип функционирования различных элементов Вооруженных Сил в едином информационном пространстве. Анализируются образцы существующего отечественного и зарубежного оборудования для обмена информационными сообщениями. На основании проведенного анализа было обнаружено, что существующая радиостанция отечественного образца не соответствует современным требованиям по защите информации. В то же время радиостанция 9681 V / UHF обеспечивает требования к полосе пропускания каналов данных и уровень безопасности. Но модернизация самолетов на базе рассматриваемой радиостанции требует значительных материальных затрат и внедрения стандартов НАТО. Анализируется статья "Способ скрытой передачи информации в голосовом сообщении". Анализ показал, что разработанный метод скрытой передачи информации в голосовом сообщении имеет недостатки, а именно: 1) недостаточную пропускную способность; 2) искажения, возникающие при переходе в частотный диапазон; 3) сложность в расчете; 4) оценка метода в условиях преднамеренного искажения не рассматривалась. Для устранения выявленных недостатков предлагается использовать помехоустойчивый код Хэмминга, который обеспечивает обнаружение и исправление ошибок, возникших при передаче голосового сообщения. На основе кодирования Хэмминга был разработан метод, позволяющий скрыть дополнительную информацию в голосовом сообщении. На основе метода разработана система прямого и обратного кодирования. Одновременно с реализацией конфиденциальности голосовых сообщений, метод дополнительно учитывает вопросы обеспечения целостности, доступности и качества информации.

Ключевые слова: *кодирование Хемминга, скрытое встраивание данных, канал передачи данных, бит.*

METHOD OF NOISELESS CODING OF VOICE MESSAGE WITH HIDDEN ADDITIONAL INFORMATION

V. Parfylo, A. Bekirov, V. Parfylo, S. Kovtunenko

The article deals with the actual question of providing a given level of information security of the Air Force aviation in the conditions of modern armed confrontation. The principle of functioning of different elements of the Armed Forces in a single information space is considered. 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 radio station 9681 V/UHF 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 article "Method of hidden transfer of information in voice message" is analyzed. The analysis revealed that the developed method of hidden transmission of information in a voice message has disadvantages, namely: 1)insufficient capacity; 2)the distortions that appear during the transition to the frequency range; 3)complexity in calculation; 4)evaluation of the method in the conditions of deliberate distortion was not considered. To remedy the identified shortcomings, it is suggested to use a fault-tolerant Hamming code, which provides for the detection and correction of errors that occurred during the transmission of a voice message. In this case, a hidden data channel is created. The extraction of embedded information is implemented on the receiving side by determining the position of the embedded bit. The restoration of the original voice message is carried out on the basis of reverse decoding with error correction. Based on Hamming's coding, a method was developed to hide additional information in a voice message. A system of direct and reverse coding was developed based on the method. Simultaneously with the realization of the confidentiality of voice messages, the method additionally takes into account the issues of ensuring the integrity, accessibility and quality of information.

Keywords: *Hamming encoding, hidden data embedding, data channel, bit.*