УДК 681.324 DOI: 10.30748/zhups.2019.60.11

А.Е. Бекіров, А.О. Краснoруцький, Н.М. Ковтуненко

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

МЕТОД ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ РАДІОПЕРЕГОВОРІВ АВІАЦІЇ

У статті розглядається актуальне питання забезпечення захищеності радіопереговорів авіації Повітряних Сил Збройних Сил України. Проводиться аналіз функціонування існуючого обладнання забезпечення конфіденційності радіообміну, формулюються основні проблемні недоліки. Пропонується напрямок забезпечення захищеності семантичної складової голосового повідомлення з врахуванням особливостей функціонування існуючого обладнання. Розробляється метод забезпечення конфіденційності радіопереговорів на основі інверсного інкрементного кодування складових спектрального представлення фрагментів мовного повідомлення при наявності ключової інформації. На основі програмної моделі проведено оцінку розробленого методу з позиції спотворень вхідного та перетвореного голосового повідомлення для авторизованого користувача та противника.

Ключові слова: *конфіденційність радіопереговорів, дельта-кодування, спектр мовного повідомлення, ключове правило.*

Вступ

Постановка проблеми. Ефективне функціонування та виконання бойових завдань повітряним компонентом Збройних Сил України безпосередньо залежить від оперативності, своєчасності та якості зв’язку. Найбільшої актуальності питання забезпечення ефективного обміну інформацією між екіпажами повітряних суден та пунктами управління набуває під час виконання завдань в умовах проведення Операції Об’єднаних Сил [1].

Аналіз останніх досліджень і публікацій. Аналіз розвитку військової техніки противника, а також досвід останніх конфліктів показав, що пріоритетним питанням для авіації є розробка та впровадження підходів щодо забезпечення інформаційної скритності обміну голосовими повідомленнями між екіпажами повітряних суден, а також пунктами управління та забезпечення вимог до ефективного радіообміну, а саме вимог оперативності, своєчасності та якості зв’язку. В першу чергу це пов’язано з активною протидією противника, а саме функціонуванням підрозділів радіо та радіотехнічної розвідки та підрозділів радіоелектронної боротьби [2]. В той же час, в умовах протистояння інформація набуває великої значимості, адже пов’язана з життям військовослужбовців.

Забезпечення зв’язку між пунктами управління та повітряними суднами Повітряних Сил (далі ПС) та Армійської авіації Сухопутних Військ Збройних Сил України (далі ЗСУ) забезпечуються штатними радіостанціями, які на сучасному етапі розвитку засобів зв’язку не завжди задовольняють вимогам щодо забезпечення конфіденційності переговорів [3]. На озброєнні авіації ПС ЗСУ перебувають аналогові радіостанції, які забезпечують симплексний двосторонній зв'язок у короткохвильовому та ультракороткохвильовому діапазоні. Найбільш розповсюдженими серед авіаційних радіостанцій є ультракороткохвильові радіостанції Р-800Л1(Л2), Р-863 (Р-862), Р-832 (Р-832М)[4].

Радіостанція Р-800Л1(Л2) встановлюється на літаку Су-27 та працює сумісно з апаратурою засекречування та апаратурою частотної телеграфії у складі типового комплексу зв’язку ТКС-2 [5]. Особливістю функціонування даної радіостанції є те, що вона забезпечує обмін інформаційними повідомленнями у цифровому вигляді у радіоканалі на основі використання частотної телеграфії. В цьому випадку голосові повідомлення перетворюються у цифровий вигляд, криптографічно перетворюються та поступають в канал передачі даних.

Наступний аналіз стану інформаційної захищеності радіопереговорів передбачає розгляд механізму засекречування голосових повідомлень на основі обладнання ТКС-2 з каналоутворюючою апаратурою на основі радіостанції Р-800Л1. Використання апаратури засекречування у типовому комплексі зв’язку ТКС-2 передбачає наступні етапи:

1. Дискретизація та квантування вихідного голосового повідомлення. Даний етап уявляю собою попередню обробку вихідного голосового повідомлення з метою представлення його у цифровому вигляді. Вихідне голосове повідомлення підсилюється та передається через апаратуру комутації П-515-1 до апаратури Т-820 де відбувається аналогово-цифрове перетворення.

2. Засекречування голосового повідомлення у цифровому вигляді [6]. В апаратурі Т-820 цифрове повідомлення ділиться на фрагменти довжиною 256 біт та кодується криптографічним блочним кодом у

відповідності із завчасно введеною ключовою інформацією.

3. Передача голосового повідомлення. Криптографічно перетворене повідомлення у двійковому вигляді передається через Р-098 “Лиман” до радіостанції Р-800Л1. У радіостанції цифрове повідомлення передається за допомогою частотної телеграфії.

Функціонування ТКС-2 у режимі забезпечення конфіденційності має деякі системні недоліки. Перший системний недолік обумовлений необхідністю чіткою синхронізації передавача та приймача. Це пояснюється тим, що на приймальній стороні втрата навіть декількох біт вхідного повідомлення може призвести до помилкового декодування всього блоку бітів і як наслідок голосового повідомлення в цілому. Така особливість роботи впливає на якість та оперативність зв’язку. Другим системним обмеженням є необхідність використання запам’ятовуючого пристрою при роботі апаратури засекречування. Це обмеження обумовлене тим, що каналоутворююча апаратура має обмежену пропускну здатність, а саме 300 бод на секунду і погіршує оперативність передачі повідомлення [7]. Тому актуальним напрямком досліджень є розробка методу забезпечення конфіденційності переговорів в умовах забезпечення заданої якості та оперативності зв’язку.

Мета статті – розробка методу забезпечення конфіденційності радіопереговорів в інтересах авіації.

Виклад основного матеріалу

Для забезпечення ефективного функціонування методу, який розробляється, сформулюємо наступні вимоги:

1. Час t_{tr} реалізації алгоритму захисту інформації має бути мінімальним. Цей показник характеризує метод з позиції часових втрат на реалізацію методу обробки голосового повідомлення.

2. Ймовірність P_{dis} розкриття противником змісту мовного повідомлення має бути найменшою, а у ідеальному випадку дорівнювати нулю:

$$P_{dis} \to 0 .$$

3. Ймовірність P_{dec} правильного декодування прийнятого голосового повідомлення має бути максимальною, тобто дорівнювати одиниці. Тут розглядається необхідність забезпечення однозначного декодування повідомлення в умовах активних впливів.

4. Полоса частот $\Delta f'$ перетвореного повідомлення має співпадати з полосою частот Δf вихідного мовного повідомлення:

$$\Delta f = f'_{\max} - f'_{\min} = f_{\max} - f_{\min} = \Delta f' .$$

5. Час t_{tr} реалізації алгоритму має дорівнювати часу t_{itr}, необхідному на реалізацію зворотного перетворення:

$$t_{tr} \approx t_{itr} .$$

6. Ступінь відмінності $\gamma(V; V')$ вихідного V і модифікованого V' мовного повідомлення на приймальній стороні для авторизованого користувача повинна бути мінімальною:

$$\gamma(V; V') \to \min ,$$

а ступінь відмінності $\gamma(V; V'')$ вихідного V і модифікованого V'' мовного повідомлення для зловмисника приймати максимальне значення.

Для розробки методу забезпечення конфіденційності радіопереговорів розглянемо вихідне мовне повідомлення V (рис. 1).

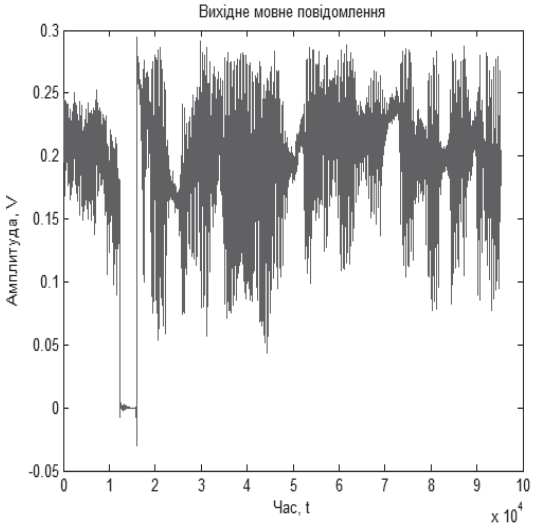

Рис. 1. Вихідне мовне повідомлення V

Для забезпечення роботи методу необхідно розділити мовне повідомлення V на фрагменти $\{V_\tau\}$, $\tau = \overline{1, L}$. Кількість таких фрагментів для вхідного голосового повідомлення V дорівнює величині L, яка розраховується на основі виразу:

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

де T – тривалість голосового повідомлення V, секунд;

t – тривалість фрагмент V_τ мовного повідомлення, секунд.

Наступний етап передбачає аналого-цифрове перетворення. Цей процес відбувається на основі дискретизації аналогового сигналу з подальшою квантизацією за рівнями амплітуди. Для забезпечення однозначного відновлення аналогової інформації необхідно забезпечити умови відповідно теореми Котельникова. В цьому випадку, для кожного безперервного сигналу з максимальною частотою

$f_{\max}$ частота дискретизації f_∂ обирається як мінімум вдвічі більшою ніж $f_{\max}$. Для голосового повідомлення V максимальне значення частоти $f_{\max}$ дорівнює 20 кГц. Отже, розрахуємо значення частоти дискретизації f_∂ та часовий інтервал між дискетами Δt:

$$f_\partial = 2 \cdot f_{\max} = 40 \quad (\text{кГц});$$

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

Операція дискретизації задається наступним виразом:

$$V_\tau = \phi_Д (V_\tau),$$

де V_τ – фрагмент мовного повідомлення V, $\tau = \overline{1, L}$;

ϕ_∂ – функціонал, який описує операцію дискретизації.

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

$$V_\tau = \{v_1; v_2; ...; v_i; ...v_M\}.$$

Наступний етап обробки фрагменту V_τ мовного повідомлення передбачає фільтрацію. Необхідність фільтрації пов'язана з особливістю обробки мовних повідомлень каналоутворюючими радіостанціями. Так для зменшення навантаження на канал передачі даних існує певний діапазон частот від $f_{c\min} = 300$ Гц до $f_{c\max} = 3400$ Гц, на яких передається мовне повідомлення [8]. Отже, в процесі передачі даних деякі складові фрагменту повідомлення після перетворення можуть бути втрачені, що в результаті призведе до втрати семантичної складової повідомлення. Оскільки ортогональні перетворення використовують задля отримання спектру сигналу, то пропонується використовувати дискретне перетворення Фур'є для визначення складових спектрального представлення фрагменту V_τ мовного повідомлення за формулою:

$$x_j = \sum_{i=1}^{N} v_i \cdot e^{-\frac{i2\pi}{N} ji},$$

де x_j – амплітуда потужності частотного спектру, яка відповідає значенню сигналу на частоті j, $j = \overline{1, I}$

v_i - i-те миттєве значення амплітуди фрагменту голосового повідомлення V_τ, $i = \overline{1, M}$.

Необхідно зазначити, що кількість складових I спектру X_τ може приймати будь-яке значення. Для визначення відповідності значення частоти j спектру до порядкового номеру складових спектрального представлення фрагменту після ДПФ проводиться наступний розрахунок:

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

Тут I – кількість частин спектрального розкладу ДПФ; f_c – необхідне значення частоти сигналу; k_c – складова спектрального представлення, яка відповідає частоті f_c. Спектральне представлення X_τ частини V_τ голосового повідомлення буде мати вигляд (рис. 2):

$$X_\tau = \{x_1; x_2; ...; x_j; ...; x_I\}.$$

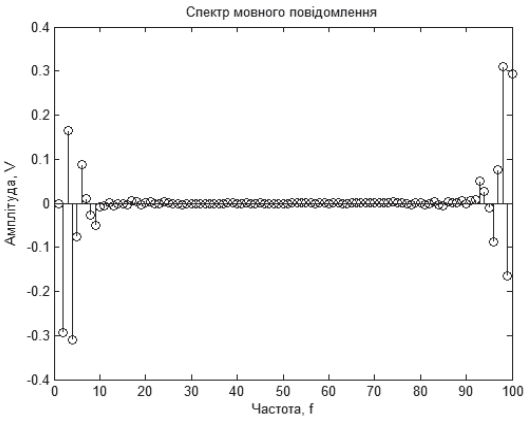

Рис. 2. Спектральне представлення X_τ частини V_τ голосового повідомлення

Тоді операція цифрової фільтрації буде виконуватись на основі системи рівнянь:

$$x'_j = \begin{cases} x_j \cdot \lambda, & \to \ j = 1...k_{c\min} \ \ \& \ \ \lambda = 0; \\ x_j \cdot \lambda, & \to \ j = k_{c\min}...k_{c\max} \ \ \& \ \ \lambda = 1; \\ x_j \cdot \lambda, & \to \ j = k_{c\max}...f_{\max} \ \ \& \ \ \lambda = 0. \end{cases}$$

Тут x'_j - j-та спектральна компонента фрагменту V_τ голосового повідомлення після операції фільтрації; λ – коефіцієнт фільтрації. Спектр X'_τ фрагменту V_τ мовного повідомлення представлено рис. 3.

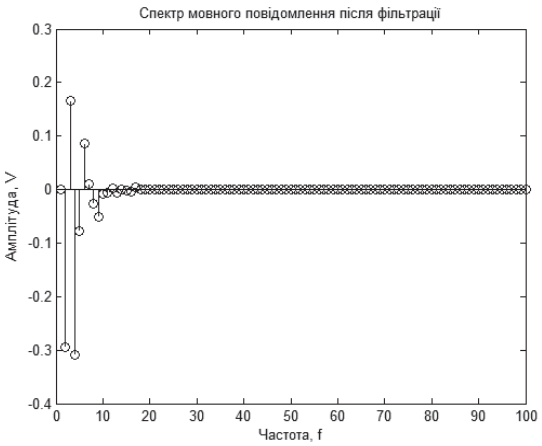

Рис. 3. Спектр X'_τ фрагменту V_τ мовного повідомлення

Схема прямого перетворення мовного повідомлення наводиться на (рис. 4).

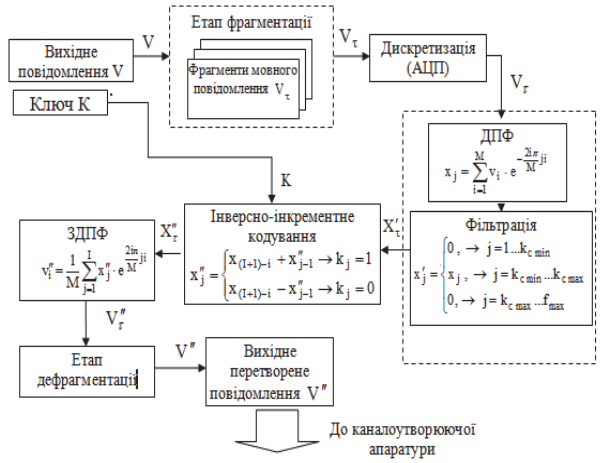

Рис. 4. Схема прямого перетворення мовного повідомлення

Наступний етап методу забезпечення конфіденційності радіопереговорів передбачає кодування складових спектру $\{x'_j\}$ фрагменту мовного повідомлення. Так, для кожної складової x'_j спектру X'_τ ставиться у відповідність значення складової x''_j модифікованого спектру X''_τ, який отримується на основі математичного функціонального перетворення. Для зменшення необхідної обчислювальної потужності задля реалізації методу одночасно з забезпеченням конфіденційності мовного повідомлення пропонується використовувати інверсно-інкрементне кодування.

Інкрементне кодування уявляє собою тип дельта-кодування, який забезпечує формування поточних кодованих елементів з урахуванням вже побудованої частини закодованого повідомлення. Іншими словами кожний кодований елемент описується функціоналом від двох аргументів, а саме поточного значення елементу та модифікованого значення попередньо кодованого елементу [9].

Для забезпечення умов щодо розділення абонентів при веденні радіопереговорів пропонується при виконанні кодування використовувати ключове правило [10]. При цьому формування модифікованого спектру на основі інкрементного кодування буде здійснюватись за інверсною схемою у відповідності до ключової інформації. В цьому випадку забезпечується збільшення ступеню відмінності між вихідною та кодованою послідовністю [11].

Реалізація інверсно-інкрементного кодування спектру X'_τ мовного повідомлення відбувається при наявності ключової інформації K. Ключова інформація $K = \{k_1, k_2 \ldots k_i \ldots k_I\}$ являє собою бітову послідовність, тобто може набувати значення $k_i \in [0,1]$ і має довжину $j = \overline{1, I}$.

Система рівняння для реалізації інкрементного кодування за інверсною схемою буде мати наступний вигляд:

$$x''_j = \begin{cases} x'_{(I+1)-j} + x'_{j-1} & \to k = 1, \\ x'_{(I+1)-j} - x'_{j-1} & \to k = 0. \end{cases}$$

На рис. 5 представлено спектр X''_τ фрагменту мовного повідомлення після модифікації.

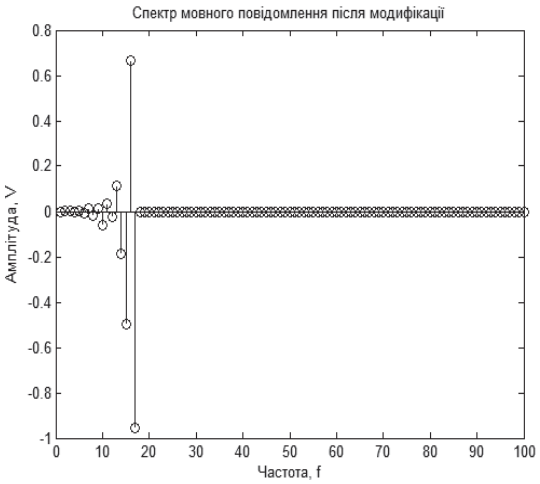

Рис. 5. Спектр X''_τ фрагменту мовного повідомлення після модифікації

Наступна обробка передбачає реконструкцію мовного повідомлення V''_τ з урахуванням модифікованого спектру X''_τ на основі зворотного перетворення Фур'є по формулі:

$$v''_i = \frac{1}{M}\sum_{j=1}^{I} x''_j \cdot e^{\frac{2i\pi}{M}ji}.$$

Фрагмент відновленого модифікованого голосового повідомлення V''_τ після зворотного дискретного перетворення Фур'є представлено на (рис. 6).

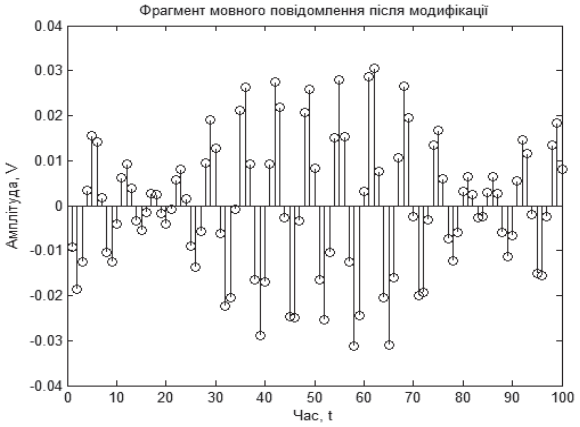

Рис. 6. Фрагмент відновленого модифікованого голосового повідомлення V''_τ після зворотного дискретного перетворення Фур'є

Остаточна композиція модифікованого голосового повідомлення V'' відбувається на основі суму-

вання всіх фрагментів $\{V''_\tau\}$, $\tau = \overline{1, L}$. Результуюче голосове повідомлення після операції цифро-аналогового перетворення має вигляд, як представлено на (рис. 7).

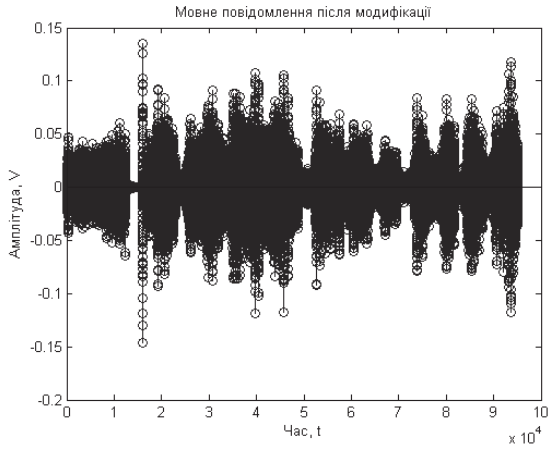

Рис. 7. Результуюче голосове повідомлення після операції цифро-аналогового перетворення

З аналізу (рис. 7) можна зробити висновок, що зовнішній вигляд модифікованого повідомлення V'' має форму, яка відрізняється від вихідного голосового повідомлення V.

Метод зворотного перетворення передбачає відновлення вихідного мовного повідомлення V на основі прийнятого каналоутворюючою апаратурою модифікованого повідомлення V'' та ключової інформації K.

Схема декодування мовного повідомлення наводиться на (рис. 8) та відбувається у зворотному напрямку.

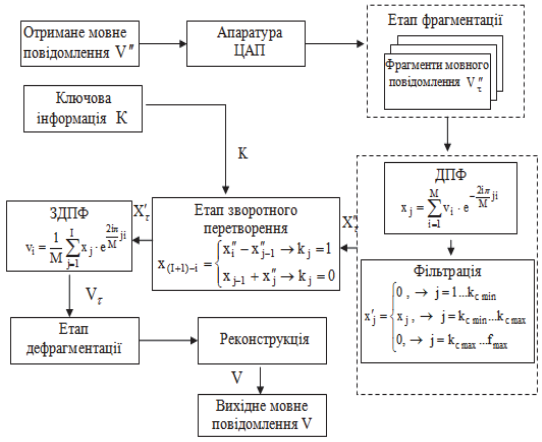

Рис. 8. Схема зворотного перетворення голосового повідомлення

У цьому випадку зворотне перетворення передбачає наступні етапи:

1. Етап фрагментації отриманого мовного повідомлення.

Вхідне повідомлення V'' з виходу каналоутворюючої апаратури поділяється на фрагменти $\{V''_\tau\}$, $\tau = \overline{1, L}$. Кількість фрагментів мовного повідомлення L приймає таке саме значення, як і у випадку прямого перетворення і визначається на основі виразу:

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

де T – тривалість голосового повідомлення V'', секунд;

t – тривалість фрагмент V''_τ мовного повідомлення, секунд.

2. Етап аналого-цифрового перетворення і фільтрації.

Для виділення полоси частот від $f_{c\min} = 300$ Гц до $f_{c\max} = 3400$ Гц, яку займає закодоване мовне повідомлення, виконується цифрова фільтрація за формулою:

$$x'_j = \begin{cases} 0, & \to j = 1...k_{c\min} \\ x''_j, & \to j = k_{c\min}...k_{c\max} \\ 0, & \to j = k_{c\max}...f_{\max} \end{cases},$$

де x''_j – значення складової спектру мовного повідомлення після дискретного перетворення Фур'є;

x''_j – значення складової спектру мовного повідомлення після фільтрації.

3. Етап декодування.

Даний етап відбувається при наявності на приймальній стороні ключової інформації $K = \{k_1, k_2...k_i...k_I\}$, яка уявляє собою бітову послідовність $k_i \in [0, 1]$ і має довжину $j = \overline{1, I}$. Декодування (зворотне перетворення) відбувається за формулою:

$$x_{(I+1)-j} = \begin{cases} x''_j - x'_{j-1} & \to k = 1; \\ x'_{j-1} + x''_j & \to k = 0. \end{cases}$$

Тут $x_{(I+1)-j}$ – отримане декодоване значення складової спектру X_τ відновленого фрагменту V_τ мовного повідомлення V.

Для отримання вихідного фрагменту V_τ для спектру X_τ виконується зворотне дискретне перетворення Фур'є.

4. Етап реконструкції мовного повідомлення [12].

Останній етап передбачає композицію вихідного мовного повідомлення V на основі декодованих фрагментів $\{V_\tau\}$ шляхом поєднання всіх фрагментів у єдину послідовність за формулою:

$$V = \sum_{\tau=1}^{L} V_\tau .$$

Відновлене мовне повідомлення V, яке містить семантичну складову передається до апаратури відтворення. У випадку відсутності або не відповідності ключової інформації мовне повідомлення буде частково або повністю знищене. Іншими словами сенс мовного повідомлення буде не доступний зловмиснику (не авторизованому користувачу). Оцінка ефективності розробленого методу виконується на основі програмної моделі алгоритму прямого і зворотного перетворення за наступними показниками:

1. Пікове відношення сигнал-шум вихідного мовного повідомлення та мовного повідомлення, відновленого в умовах авторизованого доступу при відсутності завад. Даний показник характеризує ступінь відмінності декодованого мовного повідомлення.

2. Пікове відношення сигнал-шум вихідного мовного повідомлення та мовного повідомлення, відновленого без ключової інформації (доступ зловмисника).

У якості аналого-цифрового перетворювача використовується аудіо адаптер Realtek ALC662. Оцінка методу проводиться при різних значення M кількості миттєвих значення амплітуди фрагменту V_τ мовного повідомлення та кількості I спектральних компонент дискретного перетворення Фур'є. На (рис. 9) у графічному вигляді наведені значення пікового відношення сигнал-шум модифікованого мовного повідомлення відносно вихідного сигналу для випадку неавторизованого доступу.

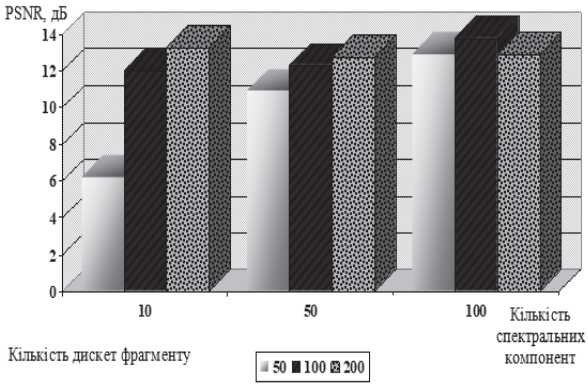

Рис. 9. Значення пікового відношення сигнал-шум модифікованого мовного повідомлення відносно вихідного сигналу

З аналізу значень (рис. 9) можна зробити наступні висновки:

– найбільше значення пікового відношення сигнал-шум спостерігається для випадку формування фрагментів мовного повідомлення з довжиною $M = 100$;

– значення пікового відношення сигнал-шум для різних умов функціонування розробленого методу приймає значення нижче порогу аудіо слухової розбірливості та відповідно забезпечує конфіденційність семантичного змісту мовного повідомлення.

Висновки

Проведено аналіз зразків радіостанцій, які є на озброєнні авіації Повітряних Сил ЗС України та існуючих підходів забезпечення конфіденційності радіопереговорів.

На основі аналізу виявлено, що розглянуті алгоритми мають системні обмеження при функціонуванні в умовах операції об'єднаних сил, а саме:

– обмежену пропускну здатність каналоутворюючої апаратури;

– необхідність синхронізації приймального та передавального обладнання.

Враховуючи обмеження застосування розглянутих алгоритмів, сформульовано вимоги щодо розробки нових підходів для забезпечення конфіденційності радіопереговорів.

Запропоновано метод прямого перетворення мовного повідомлення з використанням ключового правила, а також з урахуванням особливостей інверсно-інкрементного кодування.

Розроблено метод зворотного перетворення мовного повідомлення, який передбачає відновлення вихідного мовного повідомлення на основі прийнятого каналоутворюючою апаратурою модифікованого повідомлення та ключової інформації.

Проведено аналіз ефективності розробленого методу.

На основі аналізу встановлено, що розроблений метод забезпечує закриття семантичного змісту мовного повідомлення в умовах неавторизованого доступу (доступу зловмисника).

Список літератури

1. Досвід та особливості застосування авіації Повітряних Сил Збройних Сил України при проведенні Антитерористичної операції: довідник / В.В. Логінов, В.Ж. Ященок, В.В. Кав'юк, В.Г. Березанський, О.О. Фененко. – Х.: ХНУПС, 2016. – 34 с.

2. Алімпієв А.М. Особливості гібридної війни РФ проти України. Досвід, що отриманий Повітряними Силами Збройних Сил України / А.М. Алімпієв, Г.В. Пєвцов // Наука і техніка Повітряних Сил Збройних Сил України. – 2017. – № 2(27). – С. 19-25. https://doi.org/10.30748/nitps.2017.27.03.

3. Бурячок В.Л. Завдання, форми та способи ведення воєн у кібернетичному просторі / В.Л. Бурячок, Г.М. Гулак, В.О. Хорошко // Наука і оборона. – 2011. – № 3. – С. 35-42.

4. Наказ Міністерства оборони України "Про затвердження Правил інженерно-авіаційного забезпечення державної авіації України № 343 від 05.07.2016" [Електронний ресурс]. – Режим доступу: htpp://zakon.rada.gov.ua/laws/show/z1101-16/.

5. Седишев Ю.М. Радіоелектронні системи / Ю.М. Седишев // Міністерство освіти і науки України. – Х.: ХУПС, 2010. – 73 с.

6. Мельник А.О. Порівняльний аналіз алгоритмів стиснення мовних сигналів / А.О. Мельник, Р.П. Шевчук // Вісник. – 2004. – № 523. – С. 109-116.

7. Сучасні стеганографічні методи захисту інформації / О.І. Стасюк, С.О. Гнатюк, Н.І. Довгич, М.С. Літош // Захист інформації. – 2011. – № 1(50). – С. 151-153.

8. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення / О.К. Юдін. – К.: НАУ, 2011. – 640 с.

9. Єсін В.І. Безпека інформаційних систем і технологій / В.І. Єсін, О.О. Кузнецов, Л.С. Сорока – Х.: ХНУ ім. В.Н. Каразіна, 2013. – 632 с.

10. Бекіров А.Е. Метод захисту інформації на основі стеганографічних систем / А.Е. Бекіров // Озброєння та військова техніка. – 2015. – № 1. – С. 53-67.

11. Тарнавський Ю.А. Технології захисту інформації / Ю.А. Тарнавський // Міністерство освіти і науки України. – К.: КПІ, 2018. – 161 с.

12. 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.

References

1. Loginov, V.V., Yashhenok, V.Zh., Kav'yuk, V.V., Berezanskyj, V.G. and Fenenko, O.O. (2016), "*Dosvid ta osoblyvosti zastosuvannia aviatsii Povitrianykh Syl Zbroinykh Syl Ukrainy pry provedenni Antyterorystychnoi operatsii*" [*Information about experience of the use of military units and units of the Armed Forces of Ukraine involved in the anti-terrorist operation in the eastern regions of Ukraine*], KNAFU, Kharkiv, 34 p.

2. Alimpiiev, A.M. and Pievtsov, H.V. (2017), "Osoblyvosti hibrydnoi viiny RF proty Ukrainy. Dosvid, shcho otrymanyi Povitrianymy Sylamy Zbroinykh Syl Ukrainy" [Features of the hybrid war of the Russian Federation against Ukraine. The experience gained by the Air Force of the Armed Forces of Ukraine], *Scientific Works of Kharkiv National Air Force University*, No. 2, pp. 19-25. https://doi.org/10.30748/nitps.2017.27.03.

3. Buriachok, V.L., Hulak, H.M. and Khoroshko, V.O. (2011), "Zavdannia, formy ta sposoby vedennia voien u kibernetychnomu prostori" [Tasks, forms and methods of conducting wars in cybernetic space], *Journal of Science and Defense*, No. 3, pp. 35-42.

4. The Order of the Ministry of Defense of Ukraine (2016), "*Pro zatverdzhennya Pravyl inzhenerno-aviatsiynoho zabezpechennya derzhavnoyi aviatsiyi Ukrayiny No. 91 vid 05.07.2016*" [*On Approval of the Rules of Engineering Aviation Support of State Aviation of Ukraine No. 91 dated 05.07.2016*], available at: www.zakon.rada.gov.ua/laws/show/z1101-16/. (accessed 08 August 2016).

5. Sedyshev, J.M. (2010), "*Radioelektronni sistemi*" [*Radio electronic systems*], Kharkiv, KAFU, 73 p.

6. Melnyk, A.O. and Shevchuk, R.P. (2004), "Porivnialnyi analiz alhorytmiv stysnennia movnykh syhnaliv" [Comparative analysis of speech signal compression algorithms], *Herald*, No. 524, pp.109-116.

7. Stasiuk, O.I. (2011), "Suchasni stehanohrafichni metody zakhystu informatsii" [Modern steganographic methods of information protection], *Journal of Information Protection*, No. 1(50), pp. 151-153.

8. Yudin, O.K. (2011), "*Informatsiina bezpeka. Normatyvno-pravove zabezpechennia*" [*Informational security. Regulatory legal framework*], NAU, Kyiv, 640 p.

9. Iesin, V.I., Kuznetsov, O.O. and Soroka, L.S. (2013), "*Bezpeka informatsiinykh system i tekhnolohii*" [*Security of Information Systems and Technologies*], KNU, Kharkiv,436 p.

10. Bekirov, A.E. (2015), "Metod zashitu informacii na osnove steganografichnih sistem" [Method of protection informations on the basis of steganographic systems], *Journal of Science and Military Technics*, No. 1, pp. 53-67.

11. Tarnavskyi, Yu.A. (2018), "*Tekhnolohii zakhystu informatsii*" [*Information security technologies*], KPI, Kyiv, pp. 67-71.

12. Obod, A.A. and Strelnytskyi, A.A. (2016), "Zakhyst informatsii v merezhi system sposterezhennia povitrianoho prostoru" [Data protection in the network of observation airspace], *Information Processing Systems*, No. 2(139), pp. 47-49.

Надійшла до редколегії 11.02.2019
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

Information about the authors:

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

Красноруцький Андрій Олександрович
кандидат технічних наук старший викладач
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-4318-2217

Ковтуненко Наталія Миколаївна
бакалавр
курсант Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
www.orcid.org/0000-0003-0233-0807

Andrii Krasnorutsky
Candidate of Technical Sciences
Senior Instructor of Ivan Kozhedub Kharkiv National
Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-4318-2217

Natalii Kovtunenko
Bachelor
Cadet of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
www.orcid.org/0000-0003-0233-0807

РАЗРАБОТКА МЕТОДА ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ РАДИОПЕРЕГОВОРОВ В ИНТЕРЕСАХ АВИАЦИИ

А.Е. Бекиров, А.О. Красноруцкий, Н.М. Ковтуненко

В этой статье рассматривается актуальный вопрос обеспечения защищенности радиопереговоров авиации Воздушных Сил Вооруженных Сил Украины. Проводится анализ функционирования существующего оборудования обеспечения конфиденциальности радиообмена, формируются основные проблемные недостатки. Предлагается направление обеспечения защищенности семантической составляющей голосового сообщения с учетом особенностей функционирования существующего оборудования. Разрабатывается метод обеспечения конфиденциальности радио переговоров на основе инверсно инкрементного кодирования составляющих спектрального представления фрагментов голосового сообщения при наличии ключевой информации. На основе программной модели проведена оценка разработанного метода с позиции искажений входящего и преобразованного голосового сообщения для авторизированного пользователя и противника.

Ключевые слова: *конфиденциальность радиопереговоров, дельта-кодирование, спектр голосового сообщения, ключевое правило.*

METHOD OF AVIATION RADIO TRAFFIC CONFIDENTIALITY SECURING

A. Bekirov, A. Krasnorutsky, N. Kovtunenko

In this article we explored important question – how to provide secure aviation radio traffic of Ukrainian Air Forces. We analyzed functioning of existing radio traffic confidentiality supporting facility and formed main problems, so we proposed to support coverage of voice message semantic part with account of existing facility functioning. We are developing method which supports radio traffic confidentiality on base of inverse – increment coding of voice message spectral representation components in case of key information availability. Driven by software simulation we evaluated proposed method on the side of incoming and modified voice message distortion for authorized user and for enemy. We found out that typical communication system (TCS-2) does not correspond voice message security directives in battle situation condition. Main problem is that there is no distinct synchronization between airplane and ground command facility. Also was found out that we need to use memory storage, what causes extra channel traffic load, which has limited carrying capacity. In this article we form requirements to the method. Accomplishment of these requirements could guarantee closing of semantic component of voice message. Proposed method takes into account all system red lines of facility, which is established on the board of an airplane, and also has synchronization with other airplane, which has a key, or with ground command facility. Due to data value appraisal of modified voice message peak signal-to-noise ratio fractionally to outcome signal we made a conclusion that the data value of peak signal-to-noise ratio for different conditions of created method functioning takes a value lower then audibility cutoff and due to that provides voice message semantic content confidentiality. The use of this method on the board of an airplane in the battle allows pilot to send and receive secret information and successfully perform assigned for him mission.

Keywords: *radio traffic confidentiality, delta-coding, voice message spectrum, key rule.*