УДК 621.000 DOI: 10.30748/zhups.2020.65.12

В.А. Хлоп'ячий, А.Е. Бекіров, Н.М. Ковтуненко, О.А. Ківшар

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

МЕТОД ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ МОВНИХ ПОВІДОМЛЕНЬ НА ОСНОВІ БАГАТОВИМІРНОГО ПСЕВДОВИПАДКОВОГО БІТОВОГО РОЗПОДІЛУ

У статті розглядається актуальне питання забезпечення захисту ведення радіопереговорів Повітряних Сил Збройних Сил України. Проводиться аналіз недоліків у існуючих методах кодування мовних повідомлень. Пропонується розробка алгоритму закриття семантичної складової мовних повідомлень на основі використання багатовимірного простору, з урахуванням псевдовипадкового бітового розподілу, що містить у собі ключову інформацію. Використовуючи програмну модель, проводиться оцінка ефективності роботи методу з позиції відхилень у значеннях пікового відношення сигнал-шум для авторизованого та неавторизованого користувачів.

Ключові слова: *псевдовипадкова послідовність, тривимірна бітова площина, ключове правило.*

Вступ

Постановка проблеми. В умовах протистояння актуальності набуває питання забезпечення захисту радіообміну. В першу чергу це пов'язано з наявністю у противника сучасних засобів радіотехнічної розвідки та радіоелектронної боротьби. В той же час в умовах збройного конфлікту зростає цінність інформації, яка передається, адже вона тісно пов'язана з втратами людських і матеріальних ресурсів [1].

Аналіз останніх досліджень і публікацій. Аналіз останніх збройних конфліктів, в яких брали безпосередню участь підрозділи авіації показав, що для повітряного компоненту Збройних Сил України задача забезпечення конфіденційності радіопереговорів не вирішена повною мірою [2]. Це обумовлено тим, що існують деякі нормативно-правові обмеження впровадження нового обладнання захищених зразків, а також тим, що існуюче обладнання має певні недоліки, а саме:

– апаратура забезпечення захищеності інформації встановлена тільки на окремих типах АТ;

– наземне обладнання прийому і передачі встановлено на аеродромі (АД) базування, але відсутнє на інших пунктах управління (ПУ), що значно обмежує можливості застосування авіації, у тому числі у зоні конфлікту [3].

До того ж існуюче обладнання має ще й системні недоліки, такі як:

– застосування буферизації даних, через невелику пропускну здатність каналу передачі даних (ТКС-2 Су-27);

– наявність чіткої синхронізації передавача та приймача [4].

Існуючі методи забезпечення конфіденційності радіопереговорів мають суттєві, для ефективної роботи алгоритму, недоліки, такі як:

– складність обчислювальних ресурсів (використання ДПФ);

– перетворення аналогової інформації в цифрову, і застосування фільтрації, яка в деяких випадках може пошкоджувати семантичну складову мовного повідомлення [5].

Отже, необхідно сконцентруватися на методах, які виключають перетворення аналогової інформації в цифрову.

Мета статті – розробка ефективного методу забезпечення захищеності мовного повідомлення для передачі в штатних засобах радіозв'язку.

Виклад основного матеріалу

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

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

де T – тривалість голосового повідомлення V, секунд;

t – тривалість фрагмент V_τ мовного повідомлення, секунд [6].

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 $f_{\max}$ [7].

Операція дискретизації задається наступним виразом:

$$V_\tau = \phi_Д\left(V_\tau\right), \quad (2)$$

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

ϕ_O – функціонал, який описує операцію дискретизації.

Загальна кількість фрагментів у мовному повідомленні V представлена наступним чином:

$$V = \sum_{\tau=1}^{L} V_\tau, \ \tau = \overline{1, L}. \quad (3)$$

Наступний етап передбачає поділ існуючих фрагментів V_τ на субфрагменти. Ця операція виконується для представлення субфрагменту дійсним значенням, що в подальшому полегшує перехід в бітову послідовність. Фрагмент V_τ складає множину субфрагментів і подається такою послідовністю:

$$V_\tau = \{V_1, ..., V_i, ...V_M\}, \ i \in \overline{1; M}. \quad (4)$$

Для уникнення ймовірнісного підбору коду противником, під час роботи було вирішено застосовувати тривимірну площину, оскільки такий підхід майже унеможливлює вибір коректного ключа стороннім кореспондентом.

Кількість K елементів в кожному субфрагменті визначається на основі формули:

$$K = \frac{M}{3}, \ k = \overline{1, K}, \quad (5)$$

де M – довжина одного фрагменту.

Тоді перший субфрагмент τ-го фрагменту V_τ мовного повідомлення V буде приймати наступний вигляд:

$$Vs_\tau^{(1)} = \left\{vs_1^{(1)}, ..., vs_k^{(1)}, ..., vs_K^{(1)}\right\} = \left\{v_1, ..., v_K, ..., v_{\frac{M}{3}}\right\}, \quad (6)$$

де – $k = \overline{1, K}$.

Таким же чином формується другий і третій субфрагмент τ-го фрагменту V_τ мовного повідомлення V

$$Vs_\tau^{(2)} = \left\{vs_1^{(2)}, ..., vs_k^{(2)}, ..., vs_K^{(2)}\right\} = \left\{v_{\frac{M}{3}+1}, ..., v_K, ..., v_{\frac{2M}{3}}\right\};$$
$$Vs_\tau^{(3)} = \left\{vs_1^{(3)}, ..., vs_k^{(3)}, ..., vs_K^{(3)}\right\} = \left\{v_{\frac{2M}{3}+1}, ..., v_K, ..., v_M\right\}, \quad (7)$$

де $Vs_\tau^{(1)}$, $Vs_\tau^{(2)}$, $Vs_\tau^{(3)}$ – субфрагменти;

$vs_k^{(1)}, vs_k^{(2)}, vs_k^{(3)}$ - *k-й* елемент відповідно першого, другого та третього субфрагментів фрагменту V_τ мовного повідомлення V.

Фрагмент V_τ еквівалентний сумі субфрагментів і формується таким чином:

$$V_\tau = [Vs_\tau^{(1)}, \ Vs_\tau^{(2)}, \ Vs_\tau^{(3)}]. \quad (8)$$

Опишемо фрагмент V_τ мовного повідомлення V через суму субфрагментів:

$$V = \sum_{\tau=1}^{L} V_\tau = \sum_{r=1}^{R} Vs_\tau^{(r)} = \sum_{k=1}^{K} \cdot \sum_{r=1}^{R} vs_k^{(r)}; \ r = \overline{1, R}, \quad (9)$$

де $vs_\tau^{(r)}$ – τ-ий елемент r-го субфрагменту фрагменту V_τ мовного повідомлення.

Для переходу в бітову площину представлення мовного повідомлення пропонується записати *k-й* елемент $vs_k^{(r)}$ r-го субфрагменту фрагменту V_τ мовного повідомлення у двійковій формі. Тоді двійкове значення $bs_k^{(r)}$ елементу $vs_k^{(r)}$ отримується на основі формули:

$$bs_k^{(r)} = bit(vs_k^{(r)}), \quad (10)$$

де $bit(vs_k^{(r)})$ – функціональне перетворення для отримання двійкового значення числа.

Тоді субфрагмент $Bs_\tau^{(r)}$ в двійковій площині має наступний вигляд:

$$Bs_\tau^{(r)} = \left\{b_{k_1}^{(r)}, ..., bs_k^{(r)}, ..., bs_K^{(r)}\right\}, \quad (11)$$

де $bs_k^{(r)}$ – k-ий елемент r-го субфрагменту, який представлений у двійковому вигляді.

Кожний елемент $bs_k^{(r)}$ субфрагменту представлений множиною двійкових значень $\{c_j\}$, $j = \overline{1; J}$, а c_j може приймати значення $c \in [0; 1]$.

$$bs_k^{(r)} = \{c_j\}. \quad (12)$$

Кількість бітів J для представлення $bs_k^{(r)}$ у двійковому вигляді отримується на основі виразу:

$$J = [\log_2 vs_k^{(r)}] + 1. \quad (13)$$

Тоді значення j буде приймати вигляд:

$$j = \overline{1; J} = \overline{1; [\log_2 vs_k^{(r)}] + 1}. \quad (14)$$

Реалізація псевдовипадкової послідовності може здійснюватись на основі вибірки наступних частин мовного повідомлення, а саме:

– псевдовипадкова вибірка бітів в елементі субфрагменту;

– псевдовипадкова вибірка елементів в субфрагменті;

– псевдовипадкова вибірка площини [8].

При цьому можливе формування псевдовипадкової послідовності на основі різних правил і з різ-

ною ключовою інформацією. Тоді можливо здійснити вибірку з урахуванням:

– шляхом генерування однієї ПВП з однаковою ключовою інформацією для всіх елементів вибірки;

– за допомогою різних алгоритмів генерування ПВП з однаковими початковими даними;

– на основі генерування ПВП за різними правилами з урахуванням різних початкових параметрів;

– реалізація вибірки субфрагменту на основі генерування однієї ПВП з різними початковими даними [9].

Даний підхід забезпечує підвищення стійкості алгоритму за рахунок різних ключів, а також зменшує обчислювальну складність, що задовольняє попередньо висунутим вимогам до методу.

Для реалізації алгоритму, необхідно сформулювати правило побудови послідовності [10]. Воно може бути описане наступним чином:

$$h_\alpha = 3,9 \cdot h_{\alpha-1} \cdot (1 - h_{\alpha-1}); \overline{\alpha = 0; \infty};$$
$$h_0 = \overline{0,00(0)1 : 0,(9)9}. \qquad (15)$$

Сформоване правило дозволяє визначити позиції бітів в елементі субфрагменту, елементів у субфрагменті та у площині. Також дане правило дозволить реалізувати вибірку субфрагменту на основі генерування однієї ПВП з різною ключовою інформацією.

Нехай $H^{(J)} = \{h_1^{(J)}, ..., h_\alpha^{(J)}, ..., h_{\text{A}}^{(J)}\}$ псевдовипадкова послідовність для розподілу біт елементів субфргментів, $\alpha = \overline{1;\ \text{A}}$.

ількість елементів A псевдовипадкової послідовності $H^{(J)}$ дорівнює максимальній кількості J бітів в одному елементі субфрагменту $\text{A} = J$. Іншими словами довжина послідовності $H^{(J)}$ дорівнює кількості можливих значень, які можуть приймати значення індексів $j = \overline{1; J}$ біт в елементі субфрагменту.

Аналогічним чином визначається довжина: $\text{B} = K$ послідовності:

$$H^{(K)} = \{h_1^{(K)}, ..., h_\beta^{(K)}, ..., h_{\text{B}}^{(K)}\}$$

для розподілу елементів в субфрагменті та довжина:

$$\text{X} = R$$

послідовності:

$$H^{(R)} = \{h_1^{(R)}, ..., h_\chi^{(R)}, ..., h_{\text{X}}^{(R)}\}$$

для розподілу площин субфрагментів.

Наступний етап передбачає побудови таблиці відповідності, у якій до кожного елементу псевдовипадкової послідовності встановлюється у відповідність індекс біту (елементу, площини).

Табл. 1 побудована для розподілу індексів бітів в кожному з елементів субфрагментів.

Для кожного значення індексів $j = \overline{1; J}$ ставиться у відповідність значення елементів $\alpha = \overline{1;\ \text{A}}$ сформованої послідовності $H^{(J)}$.

Таблиця 1

Таблиця відповідності індексів бітів $j = \overline{1; J}$ і значень послідовності $H^{(J)}$

Індекси бітів	Значення послідовності
j	$h_\alpha^{(J)}$
1	$h_1^{(J)}$
2	$h_2^{(J)}$
…	…
$j-1$	$h_{\alpha-1}^{(J)}$
j	$h_\alpha^{(J)}$
$j+1$	$h_{\alpha+1}^{(J)}$
…	…
$J-1$	$h_{\text{A}-1}^{(J)}$
J	$h_A^{(J)}$

Джерело: розроблено авторами.

Аналогічним чином будуються таблиці відповідності для індексів елементів субфрагментів і мірності субфрагментів.

Враховуючи те, що всі елементи $\{h_\alpha^{(J)}\}$ приймають будь-які значення в діапазоні від 0 до 1, то наступний крок передбачає побудову табл. 2 відповідності значень індексів $j = \overline{1; J}$ і $\{h_\alpha^{(J)}\}$ у порядку збільшення значень елементів. Це дозволить сформувати послідовність розподілених значень індексів j' для псевдовипадкового перемішування бітів.

Остаточне виконання розподілу відбувається наступним чином:

$$C_{j',k'}^{(r')} = \lambda(C_{j,k}^{(r)}), \qquad (16)$$

де $C_{j,k}^{(r)}$ – j-й біт k-го елемента субфрагмента в r-й площині;

j' – положення хаотично розподіленого біту $C_{j,k}^{(r)}$ в елементі k площини r субфрагменту;

k' – позиція хаотично розподіленого елементу у субфрагменті;

r' – площина, в якій відбувається розподіл;

λ – функціональне перетворення для реалізації псевдовипадкової вибірки.

Таблиця 2

Таблиця відповідності індексів бітів $j=\overline{1;J}$ і значень послідовності $H^{(J)}$ у порядку збільшення

Значення послідовності	Індекси бітів	
$h_{\alpha}^{(J)}$	j	j'
$h_{2}^{(J)}$	2	1
$h_{\alpha-1}^{(J)}$	$j-1$	2
…	…	…
$h_{1}^{(J)}$	1	$j'-1$
$h_{A}^{(J)}$	J	j'
$h_{A-1}^{(J)}$	$J-1$	$j'+1$
…	…	…
$h_{\alpha}^{(J)}$	j	$J'-1$
$h_{(\alpha+1)}^{(J)}$	$j+1$	J'

Джерело: розроблено авторами.

На рис. 1 представлено роботу алгоритму прямого перетворення мовного повідомлення.

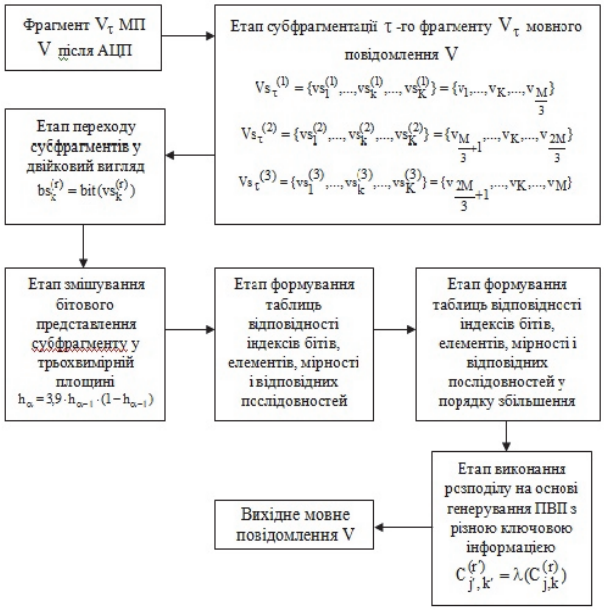

Рис. 1. Схема прямого перетворення мовного повідомлення

Джерело: розроблено авторами.

Алгоритм зворотного перетворення мовного повідомлення передбачає виконання наступних етапів:

– фрагментації вихідного мовного повідомлення V';

– аналого-цифрового перетворення фрагментів V'_τ мовного повідомлення V';

– субфрагментації τ-го фрагменту V'_τ мовного повідомлення V';

– переходу субфрагментів Vs'_τ від дійсних значень до двійкової площини;

– змішування бітового представлення субфрагменту у трьохвимірній площині.

Далі відбувається етап генерації вихідних псевдовипадкових послідовностей [11]. Для побудови правила і збору розподілених елементів мовного повідомлення в єдину інформаційну ланку, необхідно застосовувати послідовності, які здійснюють розподіл на основі генерування ПВП з різною ключовою інформацією. Нехай $H^{(J')}=\{h_1^{(J')},...,h_\alpha^{(J')},...,h_A^{(J')}\}$ псевдовипадкова послідовність для розподілу бітів прийнятого сигналу, $\alpha=\overline{1;A}$. Кількість елементів A дорівнює максимальній кількості бітів в одному елементі субфрагменту $A=J'$. Аналогічно представлено псевдовипадкову послідовність для розподілу елементів субфрагменту $H^{(K')}=\{h_1^{(K')},...,\ h_\beta^{(K')},\ ...,\ h_B^{(K')}\}$, $B=K'$ та для розподілу мірності субфрагменту $H^{(R')}=\{h_1^{(R')},...,\ h_\chi^{(R')'}\ ...,\ h_X^{(R')}\}$, $X=R'$.

Далі представлено табл. 3 відповідності елементів субфрагментів $k'=\overline{1;K'}$ і значень послідовності $H^{(K')}$.

Таблиця 3

Таблиця відповідності індексів елементів субфрагментів $k'=\overline{1;K'}$ і значень послідовності $H^{(K')}$

Значення послідовності	Індекси елементів субфрагментів
$h_\beta^{(K')}$	k'
$h_1^{(K')}$	1
$h_2^{(K')}$	2
…	…
$h_{\beta-1}^{(K')}$	$k'-1$
$h_\beta^{(K')}$	k'
$h_{\beta+1}^{(K')}$	$k'+1$
…	…
$h_{B-1}^{(K')}$	$K'-1$
$h_B^{(K')}$	K'

Джерело: розроблено авторами.

Для отримання вихідної позиції виконується зворотна операція.

В табл. 4 представлено відповідність індексів мірності субфрагментів $r' = \overline{1;R'}$ і значень послідовності $H^{(R')}$ у порядку зростання.

Завершальний етап роботи алгоритму зворотного перетворення мовного повідомлення відбувається на основі виконання остаточного розподілу, який описаний наступним чином:

$$C_{j,k}^{(r)} = \lambda^{(-1)} C_{j',k'}^{(r')}, \quad (17)$$

де $\lambda^{(-1)}$ – оператор для реалізації зворотної псевдовипадкової вибірки.

Таблиця 4

Таблиця відповідності індексів мірності субфрагментів $r' = \overline{1;R'}$ і значень послідовності $H^{(R')}$ у порядку зростання

Значення послідовності	Індекси мірності субфрагментів	
$h_\gamma^{(R')}$	r'	r
$h_2^{(R')}$	2	1
$h_{\gamma-1}^{(R')}$	$r'-1$	2
…	...	…
$h_1^{(R')}$	1	$r-1$
$h_X^{(R')}$	R'	r
$h_{X-1}^{(R')}$	$R'-1$	$r+1$
…	…	…
$h_\gamma^{(R')}$	r'	$R-1$
$h_{\gamma+1}^{(R')}$	$r'+1$	R

Джерело: розроблено авторами.

Оцінка ефективності розробленого методу виконується на основі програмної реалізації в середовищі MatLab за показниками ступеню відмінності вихідного і перетвореного повідомлення, а саме:

1. Пікове відношення сигнал-шум вхідного мовного повідомлення в умовах доступу авторизованого користувача.

2. Пікове відношення сигнал-шум вхідного повідомлення в умовах доступу неавторизованого користувача, тобто за відсутності послідовності з ключовою інформацією [12].

При тривалості голосового повідомлення $T = 5$ сек і частоті дискретизації $f_\partial = 7800$ Гц пікове відношення сигнал-шум для авторизованого користувача становить 39,5871 дБ, а для неавторизованого користувача 10,9327 дБ.

Це свідчить про те, що в умовах доступу противника, показники набувають значень нижче порогу аудіо слухової розбірливості, що відповідно забезпечує захист мовного повідомлення, яке передається.

Висновки

На основі аналізу штатного обладнання, яке є на озброєнні ПС ЗСУ виявлено, що існуюча апаратура має системні обмеження, а саме:

– застосування буферизації даних, через невелику пропускну здатність каналу передачі даних;

– необхідність наявності чіткої синхронізації передавача та приймача.

Проведено дослідження, щодо існуючих методів забезпечення конфіденційності радіопереговорів і виявлено деякі обмеження, які ускладнюють роботу алгоритмів, а саме:

– складність обчислювальних операцій (використання ДПФ);

– застосування фільтрації, яка в деяких випадках може пошкоджувати семантичну складову мовного повідомлення.

З урахуванням описаних обмежень сформульовано висновок про необхідність розробки нового алгоритму захисту мовних повідомлень на основі багатовимірного псевдовипадкового бітового розподілу. Розроблено прямий метод захисту мовних повідомлень на основі псевдовипадкової послідовності для розподілу біт в елементі, елементів в субфрагментах та площин субфрагментів.

Розроблено зворотний алгоритм захисту, який передбачає відновлення вхідного мовного повідомлення за допомогою таких самих послідовностей, які відновлюють позиції бітів. Представлено оцінку ефективності розробленого методу, на основі якого зроблено висновок про неможливість доступу зловмисника до інформації за відсутності ключа. Так значення пікового відношення сигнал-шум, яка характеризує ступінь відмінності вихідного і перетвореного мовного повідомлення забезпечується на рівні 13 дБ.

Список літератури

1. 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.

2. 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.

3. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення / О.К. Юдін. – К.: НАУ, 2011. – 431с.

4. Седишев Ю.М. Радіоелектронні системи / Ю.М. Седишев. – Х.: ХУПС, 2010. – 145 с.

5. 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.

6. Бекіров А.Е. Метод забезпечення конфіденційності радіопереговорів авіації / А.Е. Бекіров, А.О. Краснорyцький, 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.

7. Метод забезпечення конфіденційності радіопереговорів / А.Е. Бекіров, В.В. Жук, Н.М. Ковтуненко, С.Ю. Груба // Збірник тез доповідей XV Міжнародної наукової конференції "Новітні технології для захисту повітряного простору". – Харків, 11 квітня 2019 р. – С. 265-266.

8. Мартинюк Г.В. Аналіз генераторів псевдовипадкових чисел за метрологічними характеристиками / Г.В. Мартинюк, Ю.Ю. Оникієнко, Л.М. Щербак // Східно - Європейський журнал передових технологій. – 2016. – № 1/9(79). – С. 25-30. https://doi.org/10.15587/1729-4061.2016.60608.

9. Методи та засоби генерування псевдовипадкових послідовностей / Ю.І. Горбенко, Н.В. Шапочка, Т.О. Гріненко, А.В. Нейванов, Р.І. Мордвінов // Прикладна радіоелектроніка. – 2010. – № 10(2). – С. 141-152.

10. 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.

11. Горбенко Ю.І. Аналіз статистичних властивостей апаратного генератора випадкових послідовностей / Ю.І. Горбенко, Т.О. Гріненко, О.П. Нарєжній // Збірник наукових праць Харківського університету Повітряних Сил. – 2015. – № 4(45). – С. 74-77.

12. 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.

Надійшла до редколегії 29.05.2020
Схвалена до друку 14.07.2020

Відомості про авторів:

Хлоп'ячий Вячеслав Анатолійович
кандидат технічних наук
начальник факультету Харківського
національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0003-4038-9551

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

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

Ківшар Олександ Анатолійович
заступник начальника факультету
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0001-9727-7863

Information about the authors:

Vjacheslav Hlop'jachyj
Candidate of Technical Science
Chief of the Faculty of Ivan Kozhedub
KharkivNational
Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0003-4038-9551

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

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

Oleksandr Kivshar
Deputy Commander of the Faculty
of Ivan Kozhedub Kharkiv National
Air Force University
Kharkiv, Ukraine
https://orcid.org/0000-0001-9727-7863

МЕТОД ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ГОЛОСОВЫХ СООБЩЕНИЙ НА ОСНОВЕ МНОГОМЕРНОГО ПСЕВДОСЛУЧАЙНОГО БИТОВОГО РАСПРЕДЕЛЕНИЯ

В.А. Хлопячий, А.Е. Бекиров, Н.Н. Ковтуненко, А.А. Кившар

В статье рассматривается актуальный вопрос обеспечения защиты ведения радиопереговоров Воздушных Сил Вооруженных Сил Украины. Проводится анализ недостатков в существующих методах кодирования голосовых сообщений. Предлагается разработка алгоритма закрытия семантической составляющей голосовых сообщений на основе использования многомерного пространства, с учетом псевдослучайного битового распределения, которое несет в себе ключевую информацию. Предложено использование прямого и обратного методов преобразования голосового сообщения, путем избрания ключевой информации отдельно для каждой псевдослучайной последовательности, что позволит избежать вероятностного подбора противником ключа. Сформулированы правила для закрытия семантической составляющей речевого сообщения на основе представления двоичного массива исходного сообщения в многомерном пространстве. Представлено в таблицах соответствие для псевдослучайного распределения индексов битов в элементе пространственного представления, элементов в субфрагменте и индексов мерности субфрагмента .Также представлены таблицы соответствия в порядке возрастания для постановки индексов битов в элементе пространственного представления, элементов в субфрагменте и индексов мерности субфрагмента в псевдослучайном порядке. Используя программную модель проводится оценка работы метода с позиции отклонений в значениях пикового соотношения сигнал-шум для авторизированного и неавторизированного пользователей. Установлено, что при использовании метода пиковое соотношение сигнал-шум приобретает значение ниже порога аудио слуховой разборчивости для противоборствующей стороны, что говорит о эффективности работы метода.

Ключевые слова: *псевдослучайная последовательность, трехмерная битовая плоскость, ключевое правило.*

A METHOD FOR FACILITATING SECURE VOICE MESSAGES ON THE BASIS OF MULTIDIMENSIONAL PSEUDO-RANDOM BIT DISTRIBUTION

V. Hlop'jachij, A. Bekirov, N. Kovtunenko, O. Kivshar

This article deals with the topical issue of protection of conducting radio conversations of Air forces of Armed Forces of Ukraine. The analysis of the shortcomings in the existing methods of coding voice messages. It is proposed the development of an algorithm of closing of the semantic component of the voice message on the basis of using a multi-dimensional space , given a pseudo-random bit distribution, which carries key information. The proposed use of direct and inverse methods for converting a voice message by electing key information separately for each pseudo-random sequence, thereby avoiding the probability of selection of a key enemy. Defined rules for closing the semantic component of the voice message based on the representation of the binary array of the original message in a multidimensional space. Ensuring the closure of semantic meaning is carried out by multidimensional distribution of bits of the components of the original message. Pseudo-random distribution is based on constructing a dynamic sequence according to a key rule. Presented in the tables according to pseudo-random distribution of indices of bits in the element spatial representation of elements in subfragment and indices of dimensionality of subfragment .Also presents correspondence tables in ascending order for the production of indices of bits in the element spatial representation of elements in subfragment and indices of dimensionality of subfragment in pseudorandom order. Using a software model assessment method with position deviations in the values of peak signal-to-noise for authorized and unauthorized users. Found that when using the peak ratio of signal to noise assumes a value below the threshold of hearing audio intelligibility for the opposing side, which indicates the efficiency of the method.

Keywords*: pseudorandom sequence, three-dimensional bit plane, the key rule.*