УДК 629.735.05:621.396.933.43 (045)

ТЕХНОЛОГІЧНА СХЕМА ОБРОБКИ ЗАХИЩЕНОГО МОВНОГО ТРАФІКУ ІЗ ВИКОРИСТАННЯМ НЕКОГЕРЕНТНОГО ПРИЙОМУ

Веніамін Антонов

В роботі поставлено та вирішено завдання, пов'язані із створенням та оцінкою характеристик процедур некогерентного прийому вокалізованих мовних сигналів в умовах дії різноманітних дестабілізуючих факторів. Проведено аналітичні дослідження, що довели можливість застосування у вузькосмугових системах зв'язку некогерентного ЧФМ-модему, що не потребує використання пристроїв фазової синхронізації і в той же час забезпечує необхідну для нормальної роботи вокодерів швидкість та якість передавання мовного трафіку. Удосконалено технологічну схему захисту передачі параметрів вокалізованої мовної інформації через стандартний авіаційний радіоканал. Процес удосконалення полягає у заміщенні когерентної системи транспортування вокалізованих мовних сигналів некогерентним модемним зв'язком, яким не передбачено використання пристроїв фазової синхронізації і усуває причину виникнення нестабільності при організації сеансів зв'язку. В якості складового елементу вокодерної технології застосовано процедури некогерентного прийому вокалізованих мовних сигналів.

Ключові слова: *авіаційний радіозв'язок, мовний трафік, кодування, некогерентний модемний зв'язок, криптографічні алгоритми, вокодер.*

Постановка задачі. Сучасні технології передавання конфіденційної мовної інформації стандартним авіаційним радіоканалом не здатні задовольнити вимог щодо ступеню захищеності та розбірливості прийнятих мовних повідомлень за умов, коли висуваються підвищені вимоги щодо забезпечення стабільності зв'язку. Необхідні показники ефективності захисту та якості передавання мовних повідомлень у критичних авіаційних застосуваннях наразі здатні забезпечити лише вузькосмугові вокодерні системи у комбінації із стійкими криптографічними засобами і лише за умов використання когерентних систем модемного зв'язку.

Проте когерентним системам притаманний суттєвий рівень нестабільності зв'язку, що пов'язаний із роботою систем фазової синхронізації. Це обмежує використання когерентних систем передавання мовної інформації в режимі захищеного мовного діалогу через вузькосмуговий авіаційний радіоканал.

Тому у даній роботі пропонується удосконалити вокодерну технологію передачі захищеної інформації через мовний тракт авіаційного радіоканалу за рахунок використання некогерентного модемного зв'язку.

Технологічна схема обробки захищеного мовного трафіку. Проведені аналітичні дослідження довели можливість застосування у вузькосмугових системах зв'язку некогерентного ЧФМ-модему, що не потребує використання пристроїв фазової синхронізації і в той же час забезпечує необхідну для нормальної роботи вокодерів швидкість та якість передавання мовного трафіку. Тому для використання критичними прикладними застосуваннями у сфері авіаційного радіозв'язку пропонується технологічна схема захисту та передачі мовного трафіку, що показана на рис. 1. Ця схема відображає певну послідовність технологічних процесів з обробки та передавання мовної інформації через стандартний радіоканал системи авіаційного зв'язку, реалізація котрої з теоретичної точки зору забезпечує можливість надійної підтримки високоякісного зв'язку з високими рівнями конфіденційності.

Із рис. 1 видно, що для узгодження ширини спектру мовного сигналу із смугою пропускання мовного тракту стандартного авіаційного радіоканалу на передавальній стороні системи зв'язку здійснюється стиснення мовного сигналу шляхом усунення інформаційної надлишковості та «оцифровки» цього сигналу за допомогою засобів однієї із відомих вокодерних технологій. Зокрема, з цією метою доцільно використати двадцяти смуговий вокодер [1] або вокодер із лінійним провісником (ліпредер). Нестатистичне кодування алфавіту стисненого сигналу відкритої «оцифрованої» мови виконано згідно виразу (1),

$$K_U = \alpha \cdot (1 + \frac{K_м}{n_и}) \cdot (\log_2 N / \log_2 m) / \lceil \log_2 N_н / \log_2 m \rceil, \quad (1)$$

де $k_и$ – коефіцієнт нестатистичної надлишковості повідомлень; m – загальне число позицій сигналу; τ - тривалість елементарних сигналів, що відповідають певним символам коду на виході маніпуляційного кодера. Літери еквівалентного джерела повідомлень (ЕІС) (помітимо, що ЕІС складається із ІС та кодера повідомлень), що утворені послідовністю із a = 1, 2, 3, … літер ИС, кодуються рівномірним кодом із основою m.

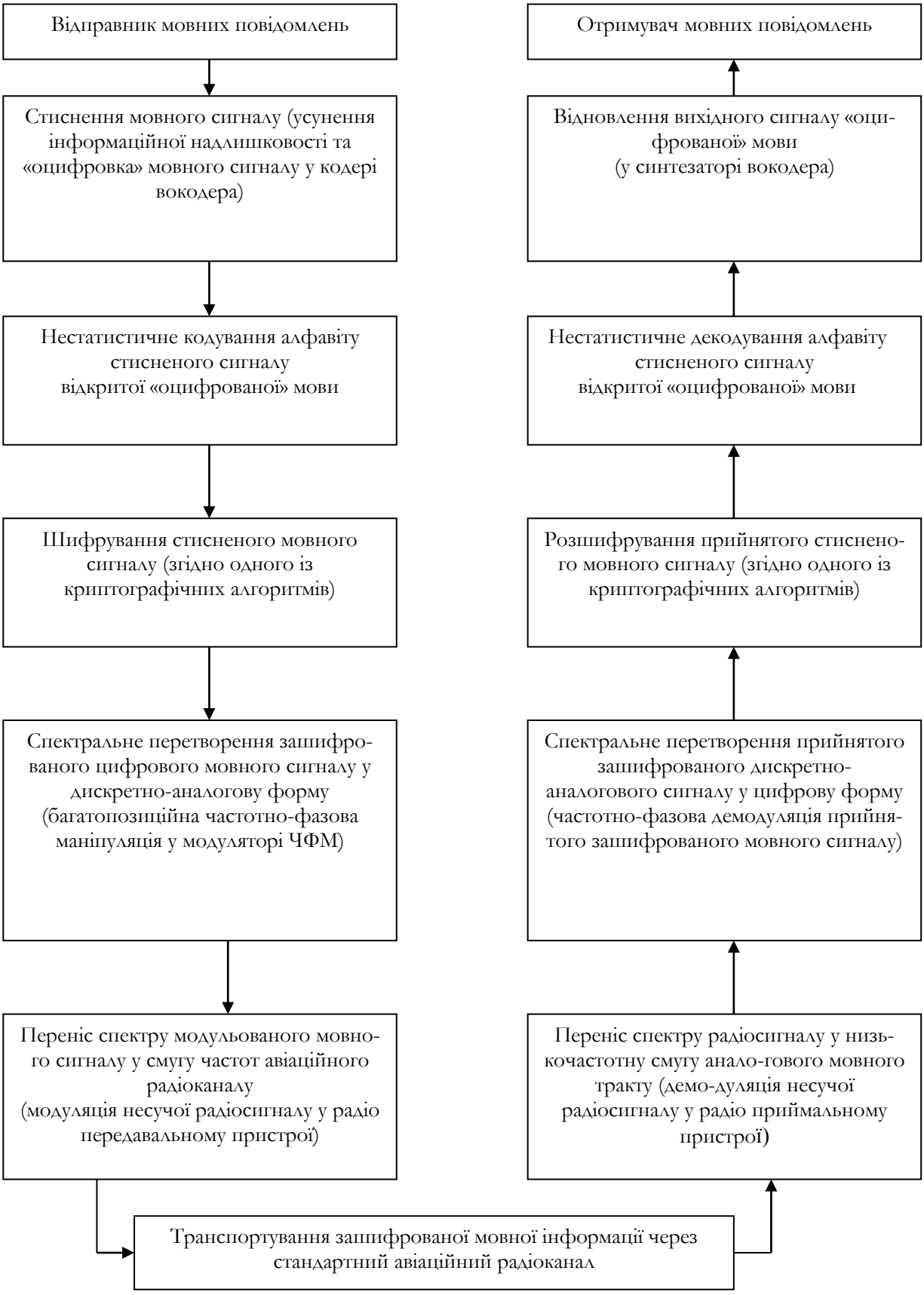

Рис. 1. Технологічна схема обробки захищеного мовного трафіку в авіаційних системах радіозв'язку

У кожній кодовій комбінації (КК) міститься

$$n = \left| \log_2 N_\chi / \log_2 m \right| \qquad (2)$$

елементарних символів, а число літер в алфавіті ЭИС дорівнює:

$$N_x = N^\alpha, \qquad (3)$$

де N – число літер в алфавіті ИС; $\lceil x \rceil$ – позначає найближче більше цілочисельне значення χ.

Коефіцієнт k_u у загальному випадку визначається як

$$K_u = (\log_2 N_x / \log_2 m) / \lceil \log_2 N_x / \log_2 m \rceil. \qquad (4)$$

З урахуванням (3) та (4) визначимо R у вигляді:

$$R = (K_э \cdot \alpha \cdot \log_2 N) / (\lceil \alpha \cdot \log_2 N / \log_2 m \rceil \ \tau \ . \qquad (5)$$

Звідкіля видно, що при N = const , τ = const та $K_э$ = const змінювання R можливо лише за рахунок змінювань α та m і в залежності від значень m R у виразі (5) має ступінчастий характер, при чому

$$\max R = K_э \cdot \alpha \cdot \log_2 N / \tau, \qquad (6)$$

досягається при

$$m = N^\alpha. \qquad (7)$$

Як видно із (7), дискретність послідовності значень N^α при α = 1, 2, 3, … є суттєвою, а спроба збільшити m супроводжується рядом труднощів, що проявляються як ускладнення обладнання, погіршення завадостійкості тощо. Якщо бажане значення m знаходиться у проміжку між N^α та $N^{\alpha-1}$, то можливе значення max R у цій ситуації не буде досягнуто.

Тому являє певний інтерес визначення такого перетворення алфавіту ИС, за котрим проміжки між можливими значеннями m, що максимізують R при $K_{ý}$ = const та τ = const, були б мінімальними. Таке перетворення реалізується у маніпуляційному кодері (МК) наступним чином (9).

На першому етапі послідовності із

$$n_{è}^{'} = n_{è} + \hat{E}_i \ , \qquad (8)$$

де $\hat{E}_i = 1 - n_{è}$, 2 - $n_{è}$,…., 0, 1, 2,… символів вихідного коду з основою m_u розглядаються як нові кодові комбінації /КК/, кількість яких дорівнює [2]:

$$N_H = \begin{cases} m_u^{n_u}, K_M \neq 0, n_u, 2n_u, ...; \\ N^{\alpha(1+K_M / n_u)}, K_M = 0, n_u, 2n_u, ...; \end{cases} \qquad (9)$$

де $K_м$ = 1- n_u , 2 - n_u ,…0, 1, 2,… – параметр МК, що дозволяє змінювати значення N_H .

Величина n_u , що входить у (8) та (9), дорівнює:

$$n_{è} = \lceil \alpha \cdot \log_2 \cdot N / \log_2 m_u \rceil. \qquad (10)$$

На другому етапі алфавіт з основою N_H у МК кодується рівномірним кодом з основою m таким чином, що кількість символів у кодовій комбінації нового коду дорівнює:

$$n_{í} = \lceil \log_2 N_{í} / \log_2 m \rceil. \qquad (11)$$

При такому процесі маніпуляційного кодування K_u визначається виразом (1).

Коефіцієнт K_u вносить певну корисну надлишковість у стиснений сигнал відкритої «оцифрованої» мови, що дозволяє підвищити можливості обміну завадостійкості на швидкість передачі інформації. Шифрування стисненого мовного сигналу здійснюється відповідно до одного із відомих криптографічних алгоритмів – блокового або потокового [3]. Наприклад, мовні компоненти кодуються у цифровий потік даних, що змішується із псевдовипадковою послідовністю, яка формується ключовим генератором згідно обраного криптографічного алгоритму.

Отримане таким чином закрите мовне повідомлення передається за допомогою некогерентного модему у канал зв'язку, на приймальному кінці котрого здійснюються зворотні перетворення з метою отримання відкритого мовного сигналу. Шляхом дискретного кодування мови з наступним її шифруванням завжди можливо досягнути ступеню закриття,що відповідає крипостійкості задіяного криптографічного алгоритму. Проте у авіаційному зв'язку цей метод не знайшов розповсюдження через низьку якість відновлення мови.

Висновки. Було вдосконалено технологічну схему захищеної передачі параметрів вокалізованої мовної інформації через стандартний авіаційний радіоканал. Процес удосконалення полягає у заміщенні когерентної системи транспортування вокалізованих мовних сигналів некогерентним модемним зв'язком, яким не передбачено використання пристроїв фазової синхронізації і усуває причину виникнення нестабільності при організації сеансів зв'язку. В якості складового елементу вокодерної технології застосовані процедури не-

когерентного прийому вокалізованих мовних сигналів. Тому в роботі поставлені та вирішені завдання, що пов'язані із створенням та оцінюванням характеристик цих процедур в умовах дії різноманітних дестабілізуючих факторів – взаємного впливу між каналами передачі, впливу імпульсних завад тощо.

ЛІТЕРАТУРА

[1]. Сапожков М.А. Вокодерная связь / М.А. Сапожков, В.Г. Михайлов – М. : Радио и связь, 1983. – 284 с.

[2]. Сервинский Е.Г. Оптимизация систем передачи дискретной информации. – М. : Связь, 1984. – 333 с.

[3]. Поточные шифры / А.В. Асосков, М.А. Иванов, А.А. Мирский и др.- М.: КУДИЦ-ОБРАЗ, 2003. - 336 с.

[4]. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М. : Издательство ТРИУМФ, 2003. – 816 с.

REFERENCES

[1]. Sapozhkov M.A. Vocoder communication, Sapozhkov M.A., Michailov V.G., M. : Radio and communication, 1983., 284 p.

[2]. Servynskyy E.G. Optimization of transmission dyskretnoy information, M. : Communications, 1984., 333 P.

[3]. Potochnye shyfry, AV Asoskov, MA Ivanov, AA Myrskyy etc., M.: KUDITS images, 2003., 336 p.

[4]. Bruce Schneier, Applied kryptohrafyya, Protocols, algorithms, yshodnыe texts in the language of Si - N: Yzdatelstvo triumph, 2003., 816 P.

ТЕХНОЛОГИЧЕСКАЯ СХЕМА ОБРАБОТКИ ЗАЩИЩЕННОГО РЕЧЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ НЕКОГЕРЕНТНОГО ПРИЕМА

В работе поставлены и решены задачи, связанные с созданием и оценки характеристик процедур некогерентного приема вокализованных речевых сигналов в условиях действия различных дестабилизирующих факторов. Проведены аналитические исследования, которые доказали возможность применения в узкополосных системах связи некогерентного ЧФМ-модема, не требуещего использования устройств фазовой синхронизации и в то же время обеспечивающего необходимую для нормальной работы вокодера скорость и качество передачи речевого трафика. Усовершенствовано технологическую схему защиты передачи параметров вокализованных речевой информации через стандартный авиационный радиоканал. Процесс усовершенствования заключается в замещении когерентной системы транспортировки вокализованных речевых сигналов некогерентной модемной связью, для которой не предусмотрено использование устройств фазовой синхронизации и устраняет причину возникновения нестабильности при организации сеансов связи. В качестве составного элемента вокодерной технологии применены процедуры некогерентного приема вокализованных речевых сигналов.

Ключевые слова: авиационный радиосвязь, языковой трафик, кодирование, некогерентный модемная связь, криптографические алгоритмы, вокодер.

FLOWSHEET PROCESSING SECURE VOICE TRAFFIC USING INCOHERENT RECEPTION

The paper raised and resolved problems related to the creation and performance evaluation procedures vokal incoherent acceptance speech signals in terms of various destabilizing factors. An analytical study proved the applicability of narrowband communication systems incoherent CHFM modem that does not require using devices of phase synchronization at the same time provides the necessary for normal functioning vocoder speed and quality transmission of voice traffic. Improved technological protection scheme parameter passing vokal voice information through a standard aircraft radio. Process improvement is the replacement of coherent transmission system vokal incoherent speech signals modem connection, which does not permit use of phase synchronization of devices and eliminates the cause of instability in the organization of sessions. As an integral element vokoder's technology applied procedures incoherent reception vokal speech signals.

Index Terms: Aircraft radio, voice traffic, coding incoherent modem connection, cryptographic algorithms vocoder.

Антонов Веніамін Валерійович, старший викладач кафедри телекомунікаційних систем Національного авіаційного університету**.**
E-mail: veniaminas@rambler.ru

Антонов Вениамин Валерьевич, старший преподаватель кафедры телекоммуникационных систем Национального авиационного университета.

Antonov Veniamin, Senior Lecturer, Department of Telecommunication Systems National Aviation University.