# КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

УДК 681.31

Б.М. ШЕВЧУК

## ОБРОБЛЕННЯ, КОДУВАННЯ ТА ПЕРЕДАВАННЯ ДАНИХ ЗАСОБАМИ АБОНЕНТСЬКИХ СИСТЕМ ІНФОРМАЦІЙНО-ЕФЕКТИВНИХ РАДІОМЕРЕЖ

*B. Chevchuk*

***PROCESSING, CODING AND TRANSFERING DATA BY USER'S SYSTEMS OF INFORMATION-EFFECTIVE RADIONETWORKS***

*Authors described information-efficient data transfer, using efficient signal processing algorithms (video), compact, crypto-resistant and anti-interference data encryption.*
*Key words: processing, coding, data transfer.*

*Описана информационно-эффективная передача данных с использованием алгоритмов оперативной обработки сигналов (видеосигналов), компактного, криптоустойчивого и помехоустойчивого кодирования данных.*
*Ключевые слова: обработка, кодирование, передача данных.*

*Описана інформаційно-ефективна передача даних з використанням алгоритмів оперативного оброблення сигналів (відеосигналів), компактного, крипостійкого та завадостійкого кодування даних.*
*Ключові слова: оброблення, кодування, передавання даних.*



Ефективне функціонування мереж передачі інформації є основою для надійної роботи комп'ютерних мереж та успішного виконання запитів і завдань віддалених абонентів (абонентських систем користувачів, різноманітних об'єктів моніторингу, виробничих автоматизованих комплексів і систем, промислових об'єктів, об'єктів екомоніторингу, транспортних засобів та ін.). Особливо це стосується абонентських систем (АС) інтегрованих комп'ютерних мереж, які не можуть бути під'єднаними до кабельних та оптоволоконних мереж зв'язку і потребують доступу до ресурсів стаціонарних мереж (Ethernet, Internet та ін.), використовуючи радіоканали. Такі мережі та системи широко використовуються в промисловості, в телемедицині, в спортивній медицині, в процесі тривалого моніторингу станів об'єктів різноманітної природи і функціонального призначення.

Для побудови безпроводових мереж на сьогоднішній день широкого розповсюдження отримали радіозасоби "останньої милі", включаючи засоби радіо-Ethernet (Wi-Fi, WiMAX), сенсорні мережі, побудовані згідно технології IEEE802.15.4 (ZigBee), радіомодулі ISM-діапазону частот різних компаній. Їх функціонування ґрунтується на використанні широкосмугових радіоканалів ISM-діапазону частот. Висока швидкість передачі інформації у таких системах досягається за рахунок використання багатопозиційних методів модуляції однієї або великої кількості ортогона-

льних несучих. Іншими прикладами успішного застосування безпроводових мереж є передача даних від рухомих та віддалених об'єктів з використанням стільникових GSM- та CDMA-мереж. Подальший розвиток радіомереж пов'язаний з розвитком когнітивних (розумних) радіосистем.

Перспективними напрямками побудови комп'ютерних мереж є інтеграція безпроводових засобів "останньої милі" з оптоволоконними мережами, створення сенсорних самоорганізуючих мереж в ISM-діапазоні частот з підвищеною надійністю зв'язку, впровадження доступних для широкого використання мікросупутникових мереж передачі моніторингових даних та ретрансляції масивів даних між віддаленими і рухомими абонентами. Для ефективного функціонування сенсорних, інтегрованих локально-регіональних та глобальних (наземно-космічних) радіомереж актуальними завданнями абонентських систем мереж є формування компактних, крипостійких та завадостійких пакетів достовірних та інформативних даних, які безконфліктно й оперативно передаються в мережах зв'язку [1, 2]. При побудові інтелектуальних об'єктних та багатофункціональних АС радіомереж ISM-діапазону частот, які встановлюються в місцях зародження та накопичення інформаційних потоків, невирішеними проблемами є оптимізація комплексу завдань, пов'язаних з введенням, обробленням, кодуванням та передаванням інформації з урахуванням обмеження на продуктивність (включаючи швидкодію і енергоспоживання) абонентських процесорів та обмеженість робочих частотних ресурсів радіоканалу. Мова йде про оптимізацію на інформаційному рівні методів і алгоритмів фільтрації та стиснення сигналів (відеосигналів), компактного, крипостійкого та завадостійкого кодування двійкових даних.

Мета роботи – розробка комплексу ефективних методів і алгоритмів оперативного оброблення, кодування та передавання різноманітних даних абонентськими системами радіомереж, включаючи відліки вимірювальних сигналів, відеосигналів (статичних та динамічних зображень), а також масивів даних. Слід зазначити, що від якості алгоритмів оброблення і кодування даних, формування канальних сигналів, які передають по радіоканалам двійкові дані та які мають бути адаптованими до поточного енергетичного співвідношення сигнал/шум у каналі зв'язку, суттєво залежать характеристики всієї мережі передачі інформації. При цьому сформовані оптимальним чином канальні сигнали за характеристиками мають відповідати поточному енергетичному співвідношенню сигнал/шум у каналі зв'язку.

**Методологічні та алгоритмічні основи реалізації інформаційно-ефективної передачі пакетів даних.** Основою для ефективного функціонування радіомереж є підтримка абонентами мережі поточної швидкості передачі інформації $R_i \to R_{\max}$ в умовах зміни співвідношення сигнал/шум у каналі зв'язку в великих межах, де $R_{\max} = 2F / k_S = 1/(T_b \cdot k_S)$; $R_{\max}$ – максимальна швидкість передачі інформації (біт/с); $F$ – величина робочої смуги частот радіоканалу (Гц); $k_S > 1.4 - 1.8$ [3] – коефіцієнт, що враховує якість відновлення фронтів цифрових

(імпульсних) сигналів; $T_b$ – тривалість двійкового символу (с). Теоретичною основою для побудови інформаційно-ефективних радіомереж є результати досліджень К. Шеннона, згідно яких при відповідних способах кодування та модуляції коефіцієнт пропускної здатності каналу зв'язку (показник інформаційної ефективності системи передачі інформації) $\eta = R / C$ [4, 5] може бути дуже близьким до одиниці ($\eta \to 1$). При цьому, згідно теорії К. Шеннона про користь кодування [4], якість передачі повідомлень можна досягти якнайкращою. Практична реалізація ідей К. Шеннона ґрунтується на побудові об'єктних та багатофункціональних АС, основою яких є високопродуктивні процесори і ПЛІС, які реалізують ефективні за точністю та швидкодією методи й алгоритми оперативного оброблення сигналів (відеосигналів), кодування та передавання пакетів даних [1, 3, 6, 7]. Оскільки каналом зв'язку вважають всі засоби та ресурси, що знаходяться між відправником і отримувачем інформації [3], то інтелектуалізація програмно-апаратних засобів АС стосується як засобів інформаційного рівня (рівня введення, оброблення, кодування та формування двійкових масивів даних і послідовностей, інтервально-імпульсних сигналів, псевдовипадкових, ортогональних, шумоподібних послідовностей) так і радіотехнічного рівня (засобів багатопозиційної модуляції, формування ортогональних несучих та піднесучих, інтелектуальних антенних систем). Основою оптимального функціонування засобів АС інформаційно-ефективних радіомереж є програмно-апаратна реалізація різноманітних за типом (функціональним призначенням) та рівнем (складністю й ефективністю відповідних методів та алгоритмів) адаптаційних процесів під час введення, оброблення, кодування та передавання інформації.

Надійна та ефективна передача інформації у радіомережах забезпечується за рахунок підтримки абонентами мережі мінімально необхідного енергетичного співвідношення сигнал/шум у радіолінії, створення умов для безконфліктної передачі інформаційних пакетів (ІП), компактного, крипостійкого та завадостійкого кодування інформаційних кадрів ІП. Досягнення максимальної поточної швидкості передачі інформації $R_i$ в радіолінії з робочою смугою частот $F$ за умови підтримки необхідного енергетичного співвідношення $(E_b / J_0)_n$ у радіоканалі ($E_b$ – енергія сигналу для одного біту (питома енергія одного біту), $J_0 = J / F >> N_0$, де $J$ – середня потужність сумарних завад у радіоканалі, $N_0$ – густина потужності шуму на один біт (спектральна густина потужності шуму)) здійснюється шляхом адаптивного вибору мінімально необхідної бази канальних сигналів $B$ з урахуванням поточного співвідношення сигнал/шум у радіоканалі [1, 2], максимального стиснення даних на інформаційному рівні та шляхом підвищення інформативності радіотехнічних засобів АС за рахунок реалізації багатопозиційних методів модуляції, передачі даних з використанням ортогональних піднесучих, використання багатопроменевих антенних систем та інші, що еквівалентно стисненню даних у процесі передачі інформації на радіо-

технічному рівні засобів АС. Для побудови портативних мережевих засобів широкого застосування (в телемедицині, спортивній медицині, АС для моніторингу віддалених промислових об'єктів, об'єктів екомоніторингу, інтелектуальних сенсорів та відеосенсорів) доцільно використовувати радіомодулі ISM-діапазону відомих компаній (SEMTECH (Xemics – DP1203F та ін.), Chipcon, Freescale, Jennic та ін.), доповнених мікроконтролерами (ARM7, ARM9, Cortex A8 та ін.), сигнальними процесорами, наприклад, сімейства Blakfin компанії Analog Devices (ADSP BF52x, 53x, 54x) та засобами формування, передавання та приймання шумоподібних сигналів з адаптивною базою ( $B = 1,..., B_{\max}$ ). При використанні шумоподібних сигналів (ШПС) швидкість передачі інформації у таких радіомережах визначається виразом [1]:

$$R_i = \frac{K_c \cdot L}{k_s \cdot T_b \cdot B}, \qquad (1)$$

де $K_c = K_i \cdot K_{rt}$ – сумарний коефіцієнт стиснення даних; $K_i$ – коефіцієнт стиснення даних на інформаційному рівні; $K_{rt}$ – коефіцієнт стиснення даних на радіотехнічному рівні; $L$ – кількість ортогональних ШПС, які асинхронно передаються в спільному радіоканалі ( $L \le B/4$ ) (величина $L$ відповідає кількості незалежних кодових моноканалів у смузі частот $F$ ).

Аналіз формули (1) показує, що при обмеженій робочій смузі частот $F$ радіоканалу та використанні спрощених радіотрактів АС (наприклад, 2–4-позиційних методів та засобів модуляції несучої) здійснення інформаційно-ефективної передачі ІП ( $R_i \to R_{\max}, \eta \to 1$ ) досягається за рахунок максимального компактного кодування даних на інформаційному рівні засобів АС, вибору мінімально необхідної бази $B_{\min}$ канальних сигналів для підтримки необхідного енергетичного співвідношення $(E_b / J_0)_n$, реалізації ефективних способів завадостійкого кодування даних ІП, паралельної передачі ІП незалежними $L$ кодовими каналами. Комплекс вимог та умов реалізації інформаційно-ефективної передачі пакетів даних описується такою системою виразів:

$$\begin{cases} P_{nc} = f(N_c, n_p) \to 1, \\ P_z = \max[2^{L_{PPi}}] \ge 2^{2048}, \\ (S/J) \cdot B_{\min} \ge (E_b / J_0)_n, \\ R^j = \dfrac{K_c \cdot L}{k_s \cdot T_b \cdot B_{\min}^j}, \\ t_{dr} + T_{ip} + T_{pk} \to t_{dr\min} + T_{ip\min} + T_{pk\min}, \end{cases} \qquad (2)$$

де $P_{nc}$ – ймовірність безконфліктної передачі пакетів інформації у процесі множинного доступу абонентів мережі до спільних ресурсів (моноканалів, абонентів); $N_c$ – максимальна кількість конфліктуючих абонентів мережі; $n_p$ – кількість рівнів пріоритетності абонентів радіомережі; $P_z$ – величина ступеня захисту інформації на АС радіомережі; $L_{PPi}$ – довжина одноразової криптостійкої псевдовипадкової послідовності, яка використовується для гаміювання компактних масивів даних; $S$ – потужність канального сигналу; $J$ – середня потужність сумарних завад у радіоканалі; $B^j_{\min}$ – мінімально необхідна база канальних сигналів для підтримки необхідного енергетичного співвідношення $(E_b / J_0)_n$ у точці прийому для $j$-го пакета; $R^j$ – максимальна швидкість передачі інформації $R^j_{\max} = I_{IP} / t_z = I_{IP} / \left(t_{dr} + T_{ip} + T_{pk}\right) R^j_{\max}$, яку визначають як кількість інформації $I_{IP}$ у бітах, що передається на протязі тривалості поточного інтервалу зайнятості каналу зв'язку $t_z$; $t_{dr}$ – інтервал доступу абонентів до спільних ресурсів мережі; $T_{ip}$ – тривалість інформаційного пакета; $T_{pk}$ – тривалість пакета-квитанції.

У залежності від наявних обчислювальних ресурсів (продуктивності центрального процесора та спеціалізованих пристроїв) на АС, ефективності алгоритмів оброблення, кодування та передавання інформації безпосередньо в місцях відбору інформації суттєво залежать базові характеристики радіомережі, включаючи надійність, якість та крипостійкість зв'язку між віддаленими АС мережі, поточна швидкість передачі інформації, особливо в умовах появи значних шумів у радіоканалі. Аналіз виразів (1) і (2) показує, що радикальним способом досягнення та підтримки інформаційно-ефективної передачі ІП у радіомережах є реалізація засобами АС максимального компактного кодування даних, включаючи фільтрацію-стиск відліків сигналів (відеосигналів) [2, 8], оперативний стиск-захист масивів даних, формування компактних, крипостійких та завадостійких ІП [1, 2]. При використанні спрощених радіотехнічних засобів інтелектуальних радіомодулів АС широкого застосування (наприклад, радіомодулів DP1203F, доповнених мікроконтролерами або сигнальними процесорами), суттєво підвищити ефективність передачі інформації можливо за рахунок оптимізації величини $K_i \to \max K_i$, де $K_i = k_1 \cdot k_2 \cdot k_3$ – сумарний коефіцієнт стиснення даних до передачі ІП та в процесі передачі ІП [1], $k_1$ – коефіцієнт стиснення даних з допустимими (контрольованими) втратами (характерний при обробці сигналів і зображень, при стиску масивів даних $k_1 = 1$); $k_2$ – коефіцієнт стиснення даних без втрат; $k_3$ – коефіцієнт стиснення даних у процесі формування та передавання ІП, величина якого у випадку використання бінарних (простих та завадостійких) схем маніпуляції досягає величин $k_3 \geq 1.6...2$ [2]. Основою перспективного

розвитку інформаційно-ефективних та когнітивних радіомереж є надвисоке стиснення даних (в десятки-сотні разів) на інформаційному рівні засобів АС, за рахунок чого суттєво зменшується кількість ІП, які відправляються до спільних ресурсів мережі, формуються крипостійкі та псевдохаотичні інформаційні кадри ІП, забезпечуються умови для внесення збитковості в канальні сигнали для підтримки необхідного співвідношення сигнал/шум у радіоканалі.

**Компактне кодування відліків сигналів та відеосигналів.** Послідовності цифрових відліків сигналів та *R*-, *G*-, *B*-відеосигналів утворюють обвідні, на яких, оперативним способом, шляхом аналізу змін знаків поточної різниці $\Delta X_i^f = X_i^f - X_{i-1}^f$ між сусідніми відліками попередньо відфільтрованих сигналів визначаються параметри екстремумів, а шляхом аналізу змін знаків поточної різниці $\Delta(\Delta X_i^f) = \Delta X_i^f - \Delta X_{i-1}^f$ між сусідніми приростами сигналів визначаються параметрами точок перегину (опуклості обвідної), де $X_i^f$ – поточний відлік відфільтрованого сигналу. Екстремуми та точки перегину є тими найбільш інформативними відліками сигналів (суттєвими відліками), параметри яких у процесі стиснення мають бути незмінними (точними) або приблизно точними, в залежності від характеристик поточних ділянок обвідної, виду компактного кодування даних [1, 2]. У залежності від функціональної орієнтації АС, галузей застосування компактне кодування відліків сигналів можливе без їх попередньої фільтрації (для точного відновлення первинних сигналів та зображень), з використанням оперативних методів фільтрації на основі ковзкого згладжування відліків сигналу з адаптивним вікном усереднення кількості відліків або адаптивної медіанної фільтрації. Вибір методу фільтрації та стиснення відліків сигналу суттєво залежить від продуктивності обчислювальних ресурсів на АС та наявного часу обробки даних. Необхідність попередньої фільтрації відліків сигналу перед їх стисненням пояснюється доцільністю отримання згладжених ділянок сигналів (гладких функцій), що в свою чергу приводить до зменшення кількості суттєвих відліків (СВ). Слід зазначити, що кожний метод фільтрації спотворює обвідну сигналу [2]. Використання широко розповсюджених методів фільтрації та стиснення сигналів і зображень з усіченням спектральних коефіцієнтів швидких ортогональних та вейвлет-перетворень призводить до того, що зі збільшенням коефіцієнта стиснення у відновленому масиві даних спостерігаються неконтрольовані спотворення амплітудно-часових характеристик СВ. При цьому різні ортогональні перетворення характеризуються своєрідними спотвореннями, які суттєво залежать від вхідного співвідношення сигнал/шум, характеристик базису та форм базисних функцій [2]. Після фільтрації сигналів із-за вхідних шумів в околиці точок перегину та екстремумів можливе виявлення декількох сусідніх СВ, тому реалізація фільтрації-стиснення відліків сигналів з контрольованими втратами суттєво залежить від прийнятої стратегії та методології фільтрації-стиснення сигналів, тобто в залежності від вибраного типу та рівня адаптації у процесі фільтрації-стиснення даних. На практиці можливі такі режими роботи програмно-апаратних засобів АС:

- компактне кодування СВ без втрат (відсутня попередня фільтрація сигналу);

- фільтрація сигналу та адаптивне кодування СВ з контрольованими втратами;

- фільтрація сигналу з найбільш максимальним компактним кодуванням СВ.

У першому режимі компактного кодування даних амплітудно-часові характеристики СВ кодуються без спотворень. У другому режимі кодування з урахуванням продуктивності абонентських процесорів, наявного часу обробки (в реальному часі, тобто в темпі введення даних, з мінімальною затримкою), рівня складності й ефективності адаптивного алгоритму фільтрації-стиснення сигналів, здійснюється компактне кодування потоку даних СВ, несуттєвих відліків (НВ) та службової інформації. Вихідні компактні потоки даних кодуються у вигляді наступного бітового потоку даних [8]: $\{ЗСІ\}[\{СІВ_i\}\{КДВ_i\}]$, де ЗСІ – загальна службова інформація, $СІВ_i$ – службова інформація $i$-ї (поточної) вибірки сигналу (відеосигналу), $КДВ_i$ – компактні дані поточної вибірки сигналу. В залежності від динамічних характеристик ділянок сигналів, вхідного співвідношення сигнал/шум службові дані $\{СІВ_i\}$ адаптивно змінюються, а послідовності амплітудних значень СВ кодуються в полі $\{КДВ_i\}$ різницевим кодом, після якого слідує код кількості НВ між сусідніми СВ. Третій режим компактного кодування сигналів (відеосигналів) орієнтований на реалізацію надвисокого стиснення даних, при цьому за рахунок адаптації здійснюється прорідження відліків сигналів, обмежується точність кодування даних, яка з точки зору дослідників (експертів) не змінює візуальні характеристики обвідної сигналу (зменшується кількість достовірних біт АЦП, зменшується кількість СВ і НВ, при цьому відповідні незначні по амплітуді СВ можуть ігноруватись, на динамічних ділянках обвідної точки перегину не виявляються).

У кінцевому рахунку основна проблема фільтрації та стиснення сигналів з допустимими втратами полягає у досягненні оптимальних характеристик процесів фільтрації-стиснення відліків сигналу при використанні відповідних процесорів та спеціалізованих пристроїв і оптимізованих за точністю і швидкодією алгоритмів попередньої обробки інформації. З метою досягнення високих коефіцієнтів стиснення даних доцільно оперативно виявляти найбільш інформативні ділянки сигналів, які кодуються найбільш точно, а на менш інформативних та зашумлених ділянках серед групи сусідніх СВ доцільно виявляти найінформативніші СВ та кодувати їх меншою кількістю біт. Відповідно, максимальний коефіцієнт стиснення даних з втратами досягається при кодуванні менш інформативних та недостовірних (вражених шумами) ділянок сигналу.

Після стиснення сигналів з допустимими втратами в масиві даних є збиткові послідовності двійкових даних, тому подальше компактне кодування вхідних масивів даних грунтується на оперативних методах стиснення двійкових послідовностей без втрат інформації. Як правило, стиснення даних без втрат є багатостадійним процесом [9], один із ефективних етапів якого є компактне кодування

даних з використанням словникових методів стиснення даних. Підвищення ефективності стиснення даних без втрат досягається за рахунок реалізації $m$-канального ($m > 1$) відбору вхідних послідовностей різної тривалості, вибором результатів кодування того каналу, який найбільш компактно кодує дані з наступним виконанням операцій заміщення двійкових послідовностей або гаміювання даних з псевдовипадковими послідовностями та виконанням наступних $n$ циклів ($n > 1$) компактного кодування даних. Багатостадійне, багатоканальне та багатоциклове компактне кодування даних може поєднуватись з захистом інформації і вимагає використання високопродуктивних процесорів.

**Криптостійке кодування масивів даних та інформаційних кадрів ІП.** Сучасні інтелектуальні радіомодулі провідних комп'ютерних та мікроелектронних компаній світу для захисту даних в ISM-діапазоні радіочастот використовують 128-бітне AES-шифрування. В роботі [10] запропоновано новий метод захисту даних у комп'ютерних мережах, згідно якого замість первинних масивів даних передаються ознаки шифрованих даних. При цьому шифрування даних грунтується на заміні байтів первинного файла байтами спеціально організованого файла-ключа.

В інтегрованих та розгалужених мережах пакети інформації від пари абонентів (відправник ІП – отримувач ІП) передаються з використанням ресурсів проміжних абонентів-ретрансляторів. Відповідно, для надійного захисту інформації у мережах тільки відповідні пари абонентів мають володіти сеансовим (поточним) секретним ключем (СК), а в пакетах інформації доступною інформацією для відповідної (обмеженої) групи абонентів має бути початок пакету та його поле адреси (часто тільки адреса отримувача ІП).

Основна проблема захисту інформації у комп'ютерних мережах полягає у розповсюдженні абонентських СК, які використовуються в процедурах аутентифікації абонентів і в шифруванні даних. Для забезпечення цілковитої секретності процесу передачі інформації необхідно, щоб при передачі кожного ІП поточний СК використовувався тільки один раз. З робіт К. Шеннона випливає, що в теоретично стійких секретних системах передачі інформації СК за обсягом не мають бути меншими, ніж обсяг первинного тексту $\{X_i\}$ та шифрограми $\{Y_i\}$. На практиці прикладом такого шифру є шифр Вернама (шифр з одноразовим ключем), причому захист інформації грунтується на виконанні операції додавання за модулем 2 над відповідними бітами масиву даних та поточного СК. Внаслідок гаміювання даних отримуємо криптограму $Y = y_1,...,y_i,...,y_n$, ($n$ – максимальна кількість біт криптограми), для якої справедливий вираз $Y = X \oplus K$, де $X = x_1,...,x_i,...,x_n$ – послідовності бітів первинного масиву даних (компактного масиву даних після виконання відповідних операцій стиснення даних), $K = k_1,...,k_i,...,k_n$ – послідовності випадкових бітів поточного СК, $y_1 = x_1 \oplus k_1,...,y_i \oplus k_i,...,y_n \oplus k_n$. Суттєвою вимогою при виконанні операцій шифрування даних з одноразовим ключем є дотримання вимоги, щоб при виконанні кожної наступної операції шифрування (гаміювання) використовувався

інший незалежно згенерований СК. Тому для *j*-ї операції гаміювання, парою абонентів, які приймають участь у передачі/прийомі ІП, генерується поточна послідовність випадкових бітів $K_j = k_j,...,k_{i+j},...,k_{n+j}$. Величина ступеня захисту інформації $P_z$ пропорційна величинам масивів даних, що підлягають гаміюванню, тобто $P_z \cong \max[2^m]$, де $m$ – мінімально необхідна довжина поточної псевдовипадкової послідовності (ПВП), яка використовується для надійного захисту поточного масиву даних ( $m \geq 2048$ біт).

Для розповсюдження та формування СК центр розподілу ключів мережі генерує випадковий сеансовий ключ для передачі поточних ІП, а далі доставляє сеансовий ключ, зашифрований за допомогою секретних ключів кожного з двох абонентів. Після дешифрування повідомлення про сеансовий ключ абоненти використовують його при передачі ІП до наступної зміни сеансового ключа. Інший, більш складніший спосіб розповсюдження ключів полягає в наступному. Кожний абонент мережі володіє закритим СК, який невідомий іншим абонентам, а також володіє базою даних кодових ключів для генерації ПВП. При необхідності передачі пакетів даних *j*-му абоненту мережі *i*-й абонент направляє йому коротке повідомлення-запит і після отримання відповіді направляє *j*-му абоненту сеансовий ключ, зашифрований засобами асиметричної криптографії. Після цього здійснюється передача ІП, зашифрованих сеансовим ключем. Більш ефективними є способи формування СК при використанні спрощених програмно-апаратних засобів з урахуванням досягнення заданої величини ступеня захисту інформації $P_z$. Для надійного шифрування даних з використанням сеансових СК здійснюється генерація відповідних ПВП та гаміювання даних після стиснення масивів даних. При наявності часу на кодування даних та при виконанні багатоциклового стиснення даних операція гаміювання може виконуватись після реалізації кожного циклу компактного кодування даних.

**Формування і передавання псевдохаотичних, криптостійких та завадостійких ІП.** Стислі та захищені масиви даних фактично є псевдохаотичними беззбитковими двійковими послідовностями, які при формуванні та передаванні ІП, трансформуються у послідовності хаотичних інтервально-імпульсних сигналів. При наявності шумів у радіоканалі, парою абонентів, у процесі встановлення зв'язку, визначаються параметри формування та прийому ШПС.

Підвищена завадостійкість передачі інформації при низькому співвідношенні сигнал/шум у радіоканалі досягається за рахунок реалізації завадостійкого кодування та перемішування даних, шляхом передачі шумоподібних ІП з оперативно визначеною мінімально необхідною базою. Перспективним способом завадостійкого кодування даних ІП є застосування рекурсивного кодування послідовностей бітів ІП з використанням кодів поля Галуа та формування сигнальних коректуючих послідовностей, які передаються в радіоканалі [11, 12]. Виявлення помилок на прийомній стороні грунтується на виконанні абонентом-відправником ІП біт-орієнтованої нумерації послідовності нулів і одиниць, які передаються за допомогою кодових послідовностей Галуа. При виявленні поми-

лок рекурентним шляхом визначається місцезнаходження того символу, який потребує виправленню. Таким чином пари АС мережі, які отримали доступ у радіоканал, з використанням сеансових СК та шляхом контролю поточного стану радіоканалу забезпечують формування криптостійких та завадостійких ІП на основі трансформації компактних масивів даних у хаотичні дані з використанням описаних процедур формування криптостійкого керованого хаосу.

**Висновки.** Запропонована технологія багатофункціональної, оперативної та адаптивної обробки та кодування даних на АС є основою для побудови когнітивних радіомереж широкого застосування для надійної та ефективної передачі інформації. При цьому дані в каналі зв'язку передаються у вигляді криптостійкого та завадостійкого хаосу, тобто хаотичною послідовністю канальних сигналів, які маскуються в шумах радіоканалу.


1. *Шевчук Б.М.* Моделі та методи обробки, кодування і передачі інформації для побудови інформаційно-ефективних комп'ютерних мереж // Комп'ютерні засоби, мережі та системи. – 2009. – № 8. – С. 81 – 89.
2. *Шевчук Б.М., Задірака В.К., Гнатів Л.О., Фраєр С.В.* Технологія багатофункціональної обробки і передачі інформації в моніторингових мережах. – К.: Наук. думка, 2010. – 370 с.
3. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение, 2-е изд.: Пер. с англ. – М.: Издательский дом "Вильямс", 2003. – 1104 с.
4. *Урядников Ю.Ф., Аджемов С.С.* Сверхширокополосная связь. Теория и применение. – М.: СОЛОН-Пресс, 2005. – 368 с.
5. *Зюко А.Г., Кловский Д.Д., Назаров М.В., Финк Л.М.* Теория передачи сигналов. – М.: Радио и связь, 1986. – 304 с.
6. *Шахнович Н.В.* Современные технологии беспроводной связи, 2-е изд.: – М.: Техносфера, 2006. – 288 с.
7. *Новые* алгоритмы формирования и обработки сигналов в системах подвижной святи / А.М. Шлома, М.Г. Бакулин, В.Б. Крейнделин, А.П. Шумов; Под ред. А.М. Шломы. – М.: Горячая линия-Телеком, 2008. – 344 с.
8. *Шевчук Б.М., Фраєр С.В.* Інститут кібернетики імені В.М. Глушкова НАН України. Спосіб фільтрації та стиску аналогового сигналу. Заявка на патент України а201006745, G 08C 19/28. Пріоритет від 01.06. 2010. – 10 с.
9. *Сэломон Д.* Сжатие данных, изображений и звука. – М.: Техносфера, 2004. – 368 с.
10. *Алишов Н.И., Марченко В.А., Оруджева С.Г.* Косвенная стеганография как новый способ защиты компьютерных данных // Комп'ютерні засоби, мережі та системи. – 2009. – № 8. – С. 105 – 112.
11. *Николайчук Я.М., Гринчишин Т.М., Заставний О.М., Воронич А.Р.* Дослідження ефективності формування сигнальних кодів // Комп'ютерні системи та компоненти. – Науковий вісник Чернівецького університету, 2009. – Вип. 479. – С. 114 – 125.
12. *Николайчук Я.М., Воронич А.Р., Гринчишин Т.М.* Теоретичні основи, принципи формування та передавання інформації на основі сигнальних коректуючих кодів // Матеріали проблемно-наукової міжгалузевої конф. "Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління (ПНМК-2010)". – Бучач: Бучачський інститут менеджменту і аудиту, 2010. – Вип. 6. – **1**. – С. 41 – 48.


Отримано 09.09.2010