2. Wagner N. R. «Searching for Public-Key Cryptosystems». In Proceedings of the 1984 Symposium on Security and Privacy (SSP ’84), P. 91–98. Los Alamitos, CA: IEEE Computer Society Press, 1990.
3. Magliveras S. S. «A Cryptosystem from Logarithmic Signatures of Finite Groups». In Proceedings of the 29th Midwest Symposium on Circuits and Systems, P. 972–975. Amsterdam: Elsevier Publishing Company, 1986.
4. Lempken W., Magliveras S. S., Tran van Trung and Wei W. Apublic key cryptosystem based on non-abelian finite groups. J. of Cryptology. 2009. 22. P. 62–74.

This paper presents comparative analysis of cryptographic realyzations on groups. It is shown that the construction of cryptosystems in groups requires efficient algorithm for the mapping of number to the group and feedback mapping with computationally simple operation group. To date, there is only one known implementation of a cryptosystem MST_3, built on the base of the abelian center of Suzuki group.

Key words: *logarithmic signature, cryptosystems PGM, MST_1, MST_2, MST_3.*

Одержано 16.02.2017

УДК 681.31

Б. М. Шевчук, канд. техн. наук

Інститут кібернетики імені В.М. Глушкова НАН України, м. Київ

ЗАВАДОСТІЙКА ПЕРЕДАЧА ЗАХИЩЕНИХ ПАКЕТІВ ДАНИХ В ІНФОРМАЦІЙНО-ЕФЕКТИВНИХ РАДІОМЕРЕЖАХ

З урахуванням оптимізації обчислень в процесі стиску та захисту сигналів, кадрів відеоданих та масивів даних запропонований комплексний підхід до реалізації швидкодіючого завадостійкого кодування і декодування захищених масивів даних, які передаються кодово-сигнальними послідовностями пакетів інформації з мінімально допустимою базою.

Ключові слова: *інформаційно-ефективні радіомережі, криптостійкі та завадостійкі пакети інформації, кодово-сигнальні послідовності пакетів, оптимізація обчислень в процесі кодування.*

Вступ. Широке застосування радіомереж, включаючи сенсорних, локально-регіональних, мікросупутникових, базується на побудові абонентських систем (АС), процесорні засоби яких здійснюють комплекс алгоритмів стиску, захисту вхідних масивів даних (сигналів, кадрів відеоданих), завадостійкого кодування стислих та захищених масивів даних, формування кодово-сигнальних послідовностей (КСП) інформаційних пакетів (ІП) з підвищеною інформаційною єм-

© Б. М. Шевчук, 2017

ністю [1–4, 6–8], передачі пакетів з мінімально необхідною базою КСП ІП для реалізації надійного зв'язку при наявності шумів та завад в радіоканалі [3, 5, 6]. При цьому КСП ІП передають n – бітові послідовності, де $n = \overline{2,8}$. Не вирішеними завданнями при побудові АС радіомереж широкого застосування є забезпечення надійної передачі ІП в радіоканалах з шумами, тобто передачі пакетів без повторень.

Мета роботи — підвищення ефективності та надійності передачі пакетів інформації у радіомережах на основі комплексного підходу до реалізації завадостійкого кодування і декодування захищених даних засобами АС з обмеженою обчислювальною продуктивністю. Вирішення цих завдань можливо досягти реалізацією швидкодіючих алгоритмів формування прихованих даних у стислих масивах без збільшення обсягу даних, внесення додаткових залежностей між сусідніми бітами масивів даних [8], формуванням та передачею завадостійких КСП ІП з урахування рівня поточних шумів у радіоканалі. При цьому на кожному етапі завадостійкого кодування здійснюється формування перевіркових кодів, які при декодуванні прийнятих даних додатково підтверджують достовірність прийнятих та відновлених інформаційних кадрів (ІК) пакетів.

Реалізація швидкодіючих алгоритмів комплексного завадостійкого кодування та декодування ІП. В радіомережах кожна АС перетворює вхідні масиви моніторингових даних у компактні, криптостійкі та завадостійкі масиви даних, які є основою ІК пакетів. При цьому ІП від віддалених АС через проміжні АС-роутери ретранслюються до АС, які виконують функції міжмережевої взаємодії. Тому на кожній АС, яка є джерелом пакетів, важливо організувати мінімізацію кількості передач ІП обмеженої тривалості та підвищеної інформаційної ємності [1, 3–5]. Вирішення цього завдання здійснюється на основі визначення найбільш інформативних, суттєвих відліків (СВ) сигналів та пікселів кадрів відеоданих, стиску та захисту масивів моніторингових даних [1, 7, 8], а також шляхом експрес-обробки моніторингових даних процесорними засобами АС з метою визначення найбільш інформативних масивів даних, які підлягають першочерговій передачі у віддалені сервери та бази даних. Кожний пакет, як правило, складається із синхропослідовностей, початку ІП (наприклад, унікальної послідовності бітів 01111110, яка не зустрічається в ІК), поля адреси (наприклад, 4 байти (по 2 байти адрес абонента-приймача і абонента передавача ІП)), поля керування (наприклад, 2 байти), поля ІК пакета, який вміщує основний (корисний) обсяг інформації, що підлягає передачі, перевіркового коду (ПрК), як правило 2–3 байти (CRC-коди циклічного контролю парності) та кінцевика ІП (послідовності 01111110). З метою реалізації адаптивної передачі пакетів довжина ІК може бути змінною,

наприклад, відповідати таким довжинам (в бітах): 128, 256, 512, 1024, 2048, 4096 і більше. З точки зору ефективності пакетної передачі інформації, коли після передачі ІП абонент радіомережі очікує зворотне підтвердження успішної передачі ІП у вигляді короткого пакета-квитанції (ПК), доцільно вибирати ІК, довжиною одиниці-десятки тисяч біт. В цьому випадку доля службових даних не перевищує 10 %. Проте тривалі ІП є більш вразливими при дії канальних завад. Тому основою завадостійкої передачі ІП є зменшення їх тривалості (в 2–3 рази і більше) за рахунок формування КСП ІП з підвищеною інформаційною ємністю [3–6], реалізація передачі пакетів, при якій основною елементарною одиницею ІП є КСП з попередньо вибраною базою канальних сигналів. При передачі в шумах радіоканалу мова йде про формування шумоподібних КСП (КСП-ШПС) з адаптивно вибраною базою ШПС. За рахунок постійного аналізу рівня шумів у радіоканалі і адаптивного вибору мінімальної бази $B_{\min}$ КСП ($B_{\min} = 1$, $B_{\min} \geq 1$, $B_{\min} > 10$) двома абонентами, що ведуть передачу пакетів, досягається підтримка необхідного енергетичного співвідношення сигнал/шум у радіоканалі [5, 7, 8]. Додатковим кодуванням для підвищення завадостійкості передачі ІП є внесення попередньої залежності між бітовими послідовностями поточних КСП та сигнальними ознаками, які передаються на модулятор (маніпулятор) радіопередавача АС [2], формування і передача КСП ПрК ІП з підвищеною базою, перемішування даних у процесі формування КСП групи ІП з метою боротьби з пакетами помилок, коли канальними завадами вражається переважна більшість КСП одного і більше пакетів, внесення додаткових залежностей між групою сусідніх бітів масиву даних [8], використання апріорної інформації, закладеної у стислі та зашифровані масиви даних, використання прихованої нумерації СВ сигналів та кадрів відеоданих, передача ІП з попередньо відомою кількістю КСП або з фіксованим обсягом інформації, формування проміжних ПрК на кожному етапі кодування даних до передачі ІП (після стиску даних з допустимими втратами, після стиску-захисту даних без втрат, після перемішування даних, після кодування з внесенням залежностей між групою сусідніх бітових даних, після формування КСП ІП), використання ефективних та швидкодіючих алгоритмів завадостійкого кодування даних з метою боротьби з одиничними та багатократними помилками, виявлених на приймальній стороні [9–12]. Слід зазначити, що для надійного прийому КСП ІП у шумах радіоканалу, окрім КСП ПрК ІП, з підвищеною базою передаються КСП початку та поля керування ІП.

Як правило, після передачі ІП деякі КСП ІП із-за дії потужних імпульсних завад можуть бути спотвореними, тобто на певних часових інтервалах ІП неможливо буде визначити тип одиночних КСП або групи

сусідніх КСП. При наявності відповідних достовірно прийнятих КСП сусідніх пакетів та їх ПрК після зворотної операції перемішування даних певні КСП будуть відновлені. У випадку використання додаткового алгоритму завадостійкого кодування зменшується кількість невизначених (невірно прийнятих) КСП. В подальшому методом перебору допустимих комбінацій невизначених бітових послідовностей ІК пакетів з використання ПрК визначаються ті масиви даних ІК ІП, як є найбільш ймовірно достовірними. Слід зазначити, що із-за обмеженої довжини ПрК ІП кількість відновлених масивів може бути значною (пропорційною відношенню довжини ІК до довжини ПрК). Визначення одного єдиного достовірно прийнятого масиву ІК із сукупності визначених масивів досягається на етапах аналізу взаємозв'язків між сусідніми бітами ІК та достовірного відновлення даних після їх стиску.

В процесі стиску сигналів з допустимими (контрольованими) втратами інформації здійснюється оперативне визначенням амплітудно-часових (номерних) параметрів найбільш інформативних СВ. Після фільтрації у процесі оперативної обробки і кодування сигналів на основі аналізу знаків різницевих значень ΔX_i^F і $\Delta(\Delta X_i^F)$ визначаються амплітудно-часові параметри СВ обвідних сигналів, де $\Delta X_i^F = X_i^F - X_{i-1}^F$ — поточний приріст сусідніх відліків X_i^F і X_{i-1}^F відфільтрованого сигналу, $i = \overline{1, v}$ — нумерація вхідних відліків поточної вибірки сигналу, v — максимальна кількість відліків, які накопичуються в оперативній пам'яті процесорного модуля АС. В залежності від оперативно визначених опосередкованих оцінок вхідного співвідношення сигнал/шум в околиці СВ $\Delta X_{CBi}^N = \left| X_{CBi}^N - X_i \right|$ та в залежності від умов $\Delta X_{CBi}^N \le \delta_d^N$ або $\Delta X_{CBi}^N > \delta_d^N$, де $\Delta X_{CBi}^F = \left| X_{CBi}^F - X_i \right|$ — оперативно визначена оцінка показника вхідного співвідношення сигнал/шум для i-го відфільтрованого СВ X_{CBi}^F, X_i — амплітудне значення вхідного сигналу, часовий відлік якого відповідає СВ X_{CBi}^F, формуються стислі масиви різницевих амплітудно-часових параметрів СВ сигналів. Чистою від шумів вважається ділянка сигналу, яку утворюють два і більше сусідніх СВ, для яких виконується умова $\Delta X_{CBi}^N < \delta_d^N$. Стислі вибірки сигналів утворюють послідовності ділянок сигналів, чистих від шумів (достовірних ділянок сигналів), або ділянок сигналів, спотворених шумами (менш достовірних ділянок сигналів). На основі адаптації кодування вхідних даних у залежності від якості введення даних (достовірні/менш достовірні ділянки сигналів), здійснюється точне (з більшою кількістю біт АЦП $q_{\max}$) або

менш точне (з меншою кількістю біт АЦП $q_{\min}$) кодування амплітудних параметрів СВ сигналів. З метою прихованого обліку стислих даних СВ (різницевих часових і амплітудних кодів) чистих ділянок і ділянок з шумами здійснюється сумування за модулем два (гаміювання) відповідної кількості біт (від одного до мінімально допустимої величини бітів амплітуд і (або) часу) поточного СВ з відповідною кількістю біт псевдовипадкової послідовності (ПВП), правила генерації якої відомі абонентам, що приймають участь у передачі і прийомі ІП. Аналогічна процедура здійснюється в процесі стиску даних без втрат, тобто певні бітові послідовності стислих даних гаміюються з відповідними бітами окремо генерованої ПВП. При відновленні даних здійснюються зворотні гаміювання та аналізуються перевіркові коди. В процесі стиску даних без втрат дані підлягають криптозахисту [7]. Алгоритм криптостійкого кодування даних, що передаються з відкритих радіоканалів, побудований на основі двоключової криптографії з використанням схеми шифрування Ель-Гамаля на еліптичних кривих. При цьому асиметрична криптографія з заданим ступенем захисту інформації забезпечує шифрування правил генерації кодових ключів, які використовуються для формування абонентських сеансових шифрів та вибору великої кількості параметрів формування КСП ІП.

Завадостійка передача ІП з внесення попередньої залежності між бітовими послідовностями та сигнальними ознаками канальних сигналів здійснюється характерною розбивкою даних ІП на n-бітові послідовності, де $n \geq 2$. За кожною поточною n-бітовою послідовністю, номер якої відповідає порядковому номеру із таблиці алфавіту всіх можливих послідовностей, закріплюється поточний одиничний або нульовий біт відповідної (попередньо генерованої) ПВП, кодові ключі генерації якої відомі абоненту-відправнику та абоненту-приймачу ІП. При цьому в процесі формування та передавання ІП закріплений поточний біт ПВП кодується (заміщується) відповідною сигнальною ознакою, яка визначає форму поточної КСП та передається на модулятор радіопередавача ОС. Необхідна кількість псевдовипадкових послідовностей G_m відповідає максимальній кількості m n-бітових послідовностей таблиці алфавіту, а необхідна кількість сигнальних ознак дорівнює $2m$. Мінімально необхідна кількість біт (довжина) псевдовипадкових послідовностей вибирається достатньою для підрахунку кожної із m n-бітових послідовностей у заданому масиві псевдохаотичних даних, що підлягають передачі. Для масиву, довжиною L біт, кількість біт l псевдовипадкових послідовностей, що використовуються для підрахунку n-бітових послідовностей вибирається, наприклад, з урахуванням, щоб $l > L / m$. Додат-

кове використання коротких ПрК забезпечує оперативне визначення групи спотворених КСП ІП шляхом перебору допустимих варіантів відповідних вражених шумами бітових послідовностей ІК пакетів.

Висновки. В радіомережах з пакетною передачею інформації основою завадостійкої передачі даних є формування і передача КСП ІП, інформаційна ємність яких, тривалість та база адаптивно підбирається абонентами в залежності від поточного енергетичного співвідношення сигнал/шум. Подальше виправлення помилок, які виникають в результаті враження канальними завадами КСП ІП, забезпечується внесенням додаткової прихованої інформації в стислі масиви даних, внесенням залежностей між групою сусідніх бітів ІК, перемішуванням даних, які передаються різними пакетами та формуванням основних (після стиску даних з допустимими втратами інформації і при формуванні та передачі КСП ІП) і додаткових перевіркових кодів.

Список використаних джерел:

1. Shevchuk B., Ivakhiv O., Geraimchuk M., Brayko Y. Efficient Encoding and Trasmission of Monitoring Data in Information-efficient Wireless Networks. The 3rd IEEE International Symposium on Wirelless Systems within the Conferences on Inteligent Data Asquisition and Advanced Computing Systems (IDAACS-SWS 2016), 26–27 September 2016, Offenburg, Germany. P. 138–143.
2. Nykolaychuk Y.M., Shevchyuk B.M., Voronych A.R., Zavediuk T.O., Glagyuk T.O. Theory of Reliable and Secure Data Transmission in Sensory and Local Area Networks. *Cybernetics and Systems Analysis.* 2014. March, Vol. 50, Is. 2. P. 304–315.
3. Shevchuk B. M. Speed and Coding Accuracy-Optimal Methods and Algorithms to Increase the Information Efficiency of the Operation of Wireless Network Subscriber Systems. *Cybernetics and Systems Analysis*. 2014. November. Vol. 50, Is. 6. P. 945–955.
4. Shevchuk B.M. Theoretical and Algorithmic Foundations of Improving the Efficiency of Packet Data Transmission in High-Speed and Secure Radio Networks. *Cybernetics and Systems Analysis*. 2016. January. Vol. 52, Is. 1. P. 151–159.
5. Shevchuk B.M. Speed-Efficient Algorithms for Transmitting and Receiving High-Informative Packets in Radio Networks. *Cybernetics and Systems Analysis*. 2016. March. Vol. 52. Is. 2. P. 330–337.
6. Шевчук Б. М., Задірака В. К., Фраєр С. В. Підвищення ефективності передачі інформації в моніторингових мережах на основі оптимізації обчислень в процесі кодування даних засобами об'єктних систем сенсорних мереж. *Управляющие системы и машины*. 2015. № 3. С. 65–71.
7. Шевчук Б. М., Задірака В. К., Фраєр С. В. Алгоритмічні основи підвищення інформаційної ефективності передачі даних в сенсорних мережах. *Комп'ютерні засоби, мережі та системи*. 2013. № 12. С. 140–149.
8. Шевчук Б. М. Системний підхід до вирішення проблем оптимізації обчислень засобами об'єктних систем сенсорних мереж. *Інформаційні технології та комп'ютерна інженерія.* 2013. № 1. С. 88–95.

9. Скляр Б. Цифровая связь. Теоретические основы и практическое применение: 2-е изд.: Пер. с англ. М.: Издательский дом «Вильямс», 2003. 1104 с.
10. Шлома А. М., Бакулин М. Г., Крейнделин В. Б., Шумов А. П. Новые алгоритмы формирования и обработки сигналов в системах подвижной связи. М.: Горячая линия-Телеком, 2008. 344 с.
11. Кичак В. М., Тромсюк В. Д. Оцінювання бітових помилок при різних видах демодуляції дискретних сигналів. *Вісник Національного технічного університету України «КПІ»*. 2015. № 63. С. 55–63.
12. Яцків В. В. Виявлення та виправлення багатократних помилок на основі медулярних коректуючи кодів. *Інформаційні технології та комп'ютерна інженерія*. 2015. № 2. С. 77–82.

Considering the calculation optimization in the compression and protection processes of signals, video data frames and data arrays it is proposed a complex approach to implementing of high-speed noise-immune coding and decoding of the protected data arrays that are transmitted by code-signal sequences of the information packets with minimum admissible base.

Key words: *information-effective radio, noise stability information package, code-signal sequence packets, optimization calculations during encoding.*

Одержано 01.03.2017