УДК 681.3

О. Л. Яковенко

ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ

Розглянуто методи забезпечення цілісності інформації в інформаційно-комунікаційних системах та мережах, основні методи підвищення завадостійкості інформаційних об'єктів. Запропоновано застосування кодів, які дають можливість забезпечити виявлення та виправлення пакетів помилок значної тривалості.

Рассмотрены методы обеспечения целостности информации в информационно-коммуникационных системах и сетях, основные методы повышения помехоустойчивости информационных объектов. Предложено применение кодов, позволяющих обеспечить выявление и исправление пакетов ошибок значительной продолжительности.

Methods to ensure the integrity of information in communication systems and networks, basic methods for improving noise immunity of information objects are shown. Application of codes that enable to provide the detection and correction of error packets of substantial duration is proposed.

Ключові слова: інформаційна система, цілісність, завадостійкість, інформація, код.

Інформаційно-комунікаційні системи та мережі (ІКСМ) стали найважливішою складовою процесу використання інформаційних ресурсів суспільства.

Забезпечення цілісності інформації при її передачі по каналах зв'язку є найактуальнішою задачею в умовах глобального розвитку інформаційно-комунікаційних систем та мереж. Виникає необхідність розробки методів ефективного завадостійкого канального кодування з максимально простою реалізацією для забезпечення цілісності та вірогідності переданих даних.

Цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем або процесом. Дана властивість інформації досягається шляхом дотримання встановлених правил її обробки. Іншими словами, під цілісністю інформації розуміють відсутність в ній будь-яких спотворень (модифікацій), які не були санкціоновані її власником, незалежно від причин або джерел виникнення таких спотворень. Спотворення інформації, тобто порушення її цілісності, можливі на будь-якому етапі її циркуляції у обчислювальних мережах: при зберіганні, передачі або обробці. Причини таких спотворень можуть бути випадковими або навмисними. У свою чергу, випадкові спотворення можуть бути як природними, пов'язаними з дією природних чинників, так і штучними.

Випадкові і штучні завади є загрозами функціональним властивостям захищеності інформаційних ресурсів – їх цілісності та доступності. Надалі розглядаються задачі забезпечення цілісності інформаційних об'єктів в умовах природних впливів. Наслідком природних впливів в каналах ІКСМ є зменшення співвідношення показника сигнал/завада. Це відношення визначає вірність інформації, що визначається через ймовірність спотворень двійкових символів (біт) $P_{сп}$, а також інтенсивність цих помилок.

Задача забезпечення цілісності і доступності інформаційних ресурсів є однією з найактуальніших при розробці і експлуатації інформаційних систем і їх елементів.

Для забезпечення контролю та поновлення цілісності інформаційних об'єктів, включаючи і відновлення зруйнованої інформації, вводять надмірну інформацію – ознаку цілісності або контрольну ознаку [1].

Однією із причин виникнення спотворень є завади, викликані зовнішніми джерелами і атмосферними явищами. Складність протидії завадам полягає в безладності, нерегулярності і в структурній схожості завад з інформаційними сигналами. Тому захист інформації від спотворень і шкідливого впливу завад має велике практичне значення і є однією з серйозних проблем сучасної теорії інформаційного обміну в каналах ІКСМ.

Серед основних методів забезпечення цілісності інформації ІКСМ слід виділити застосування різного роду завадостійких кодів з виявленням помилок. Це, в свою чергу, дає можливість застосування способів передачі повідомлень з різного роду зворотним зв'язком (інформаційного – деякий аналог мажоритарного методу з багатократною передачею інформаці, зворотним прийомом і ухваленням рішення щодо правильності передачі на стороні передавача, або з вирішальним зворотним зв'язком (ВЗЗ) – багатократний, при необхідності передачі з ухваленням рішення щодо правильності передачі на стороні приймача). Недоліки таких способів забезпечення цілісності зводяться до необхідності організації другого (зворотного) каналу зв'язку, тобто до істотних матеріальних витрат, а також до збільшення часу затримки передавання інформації, який може бути неприпустимо великим, а також застосування різного роду завадостійких корегуючих кодів (ЗКК), які дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засобів виявлення і усунення спотворень [2].

Останній із способів (механізмів) забезпечення цілісності інформаційних об'єктів − із застосуванням завадостійких корегуючих кодів наразі знайшов широке застосування в стандартах стільникового зв'язку. Він не потребує зворотного каналу і забезпечує, як правило, прийнятне значення часу затримки передавання інформаційних об'єктів. Тому, чи не єдиною проблемою в цих та інших ІКСМ з використанням телефонних кабельних та радіоканалів є проблема забезпечення цілісності інформаційних об'єктів в умовах впливу навіть природних (не говорячи уже про штучні, навмисні завади) пакетних спотворень, як «коротких» (тривалістю 2...10 мс) так і особливо «довгих» (тривалістю 100…200 мс). Це є особливо актуальним і для уже згаданих систем стільникового зв'язку. Наприклад, в стандартах CDMA базовий цифровий потік розбивається на пакети тривалістю по 20 мс та подається на згорточний кодер з половинною швидкістю [3]. При цьому тривалість пакета спотворень може бути порівняною чи, навіть, значно перевищувати тривалість інформаційного пакета, що може суттєво вплинути на результативність процедур обміну інформацією.

Як вихід із таких ситуацій може розглядатися можливість збільшення тривалості інформаційних пактів із одночасним застосуванням перемежування потрібної гли-

бини та завадостійких корегуючих кодів, які були б спроможними забезпечити виявлення та виправлення пакетів спотворень значної тривалості. Як такі коди можна застосовувати узагальнені завадостійкі корегуючі коди.

Під узагальненими розумітимемо коди, призначені для виявлення (або ж виявлення і виправлення) пакетних спотворень з кратністю b, в яких використовуються алгоритми кодування і декодування, аналогічні відповідним алгоритмам двійкових кодів, але по відношенню до узагальнених b – розрядних символів.

У цих кодах початкова двійкова кодова послідовність − базове кодове слово $I_1 I_2 ... I_m$ розбивається на $n = \frac{m}{b}$ узагальнених символів (УС) – груп двійкових розрядів з розрядністю b, в яких передбачається виявлення та виправлення спотворень:

$$\underbrace{I_1 ... I_b}\ ,\ \underbrace{I_{b+1} ... I_{2b}}\ \ \dots\ \ \underbrace{I_{m-b+1} ... I_m}$$

1-й УС 2-й УС … n-й УС

Двійкові символи, що входять в одну b-розрядну групу, розглядаються як b-значний УС, який може приймати будь-яке із s значень від 0 до $(s-1)$, де $s = 2^b$.

Одним із прикладів узагальнених кодів є код умовних лишків (ЛУ-код). Теоретичною основою ЛУ-коду є теорія лишкових класів. З теорії лишкових класів відомо, що будь-яке число можна представити у вигляді набору лишків від розподілу цього числа на набір взаємно простих чисел, які мають назву основ системи числення, $-p_i$, де $1 = 1,2$, …, n, n − кількість таких основ. Вибір величини n здійснюється з умови, яка викладена нижче. Тоді: $A = \alpha_1, \alpha_2, ..., \alpha_n$, (1)

де $\alpha = A - [\frac{A}{p_i}] \cdot p_i$, а позначка $[\frac{A}{p_i}]$ означає операцію розрахунку цілої частини від дробового числа $[\frac{A}{p_i}]$.

При цьому між числом А і його представленням вираз (1) існує взаємна однозначна відповідність, якщо:

$$A \le P = \prod_{i=1}^{n} p_i \cdot$$

У цьому виразі величина Р – діапазон представлення або робочий діапазон чисел. Звернемо увагу на те, що величина α_i представляє собою групу двійкових розрядів, кількість яких не перевищує розрядності відповідної основи p_i.

Чудовою властивістю системи лишкових класів (СЛК) є те, що в неї легко вводяться властивості виявлення і виправлення спотворень. Відомо, що якщо ввести ще одну, контрольну, основу p_k, то уявлення А в розширеному діапазоні $R = P \cdot p_k$, у вигляді: $A = \alpha_1, \alpha_2, ..., \alpha_n, \alpha_k$, (2)

де α_k – лишок по основі p_k, має чудову для побудови корегуючих кодів властивість: при $p_k > p_n$ будь-яке спотворення в одному з лишків αі може бути знайденим, а при $p_k > 2 \cdot p_n \cdot p_{n-1}$, де p_n, p_{n-1} − найбільші з основ, може бути і виправленим. Це означає, що при представленні чисел у вигляді (2) створюється завадостійкий код з можливостями або виявлення спотворень, або й їх корекції.

Такий код має недолік, пов'язаний з необхідністю роботи з числами в системі числення в залишкових класах. Цей недолік достатньо просто усувається в коді умовних лишків, який вводиться таким чином.

Хай є код деякого числа А, представленого в будь-якій системі числення, зокрема позиційної, наприклад, двійкової. Для визначеності, хай це число А представлено послідовністю з нулів і одиниць. Розіб'ємо цю послідовності певним, у загальному випадку довільним, чином на n груп, як і для решти узагальнених кодів.

Як і раніше код кожної *i*-ї групи (пакета) розглядатимемо як s-значний розряд α_i, який може приймати будь-яке з s значень від 0 до $s-1$, де $s=2^b$, але умовно вважатимемо цей код лишком деякого умовного числа А по основі p_i. Оскільки величина α_i, як елемент початкового числа: $0 \le \alpha_i \le s-1$,

а як лишок від ділення А на p_i: $0 \le \alpha_i \le p_i$,

то для представлення коду будь-якої групи у вигляді лишку по основі p_i необхідно, щоб виконувалася умова: $p_i > s-1$,

інакше в групу із b розрядів може бути записаним код $\alpha_i \ge p_i$, що в лишкових класах не допустимо.

Приклад. Нехай $b=3$, $s=7$, тоді α_i може приймати значення 000, 001, 010, …, 11. При $p_i=5$ максимальне значення α_i обмежується кодом 100, тобто коди 101, 110, 111 є «неправильними». Якщо ж взяти $p_i>7$, наприклад $p_i=9$, тоді максимальне значення α_i обмежується не величиною p_i, а розрядністю групи b, тобто $\alpha_{\max}=11$.

При такому підході будь-які комбінації початкового коду числа А «вписуються» в систему числення з основам $p_i(i=1,2,...)$. Якщо розширити систему основ на контрольну p_k і для одержаного набору умовних лишків $\alpha_i(i=1,2,...)$ розрахувати умовний лишок α_k, то на одержане умовне число: $A=\alpha_1,\alpha_2,...,\alpha_{n1},\alpha_k$ (3)

розповсюджує можливості СЛК по виявленню і виправленню спотворень, тобто одержаний код (3) має всі властивості коду (2), але останній код може бути отриманим для будь-якої двійкової послідовності, а не тільки щодо чисел в лишкових класах. Відзначимо, що таким чином усунений перший недолік коду (2).

Оскільки для отримання контрольної ознаки, тобто для кодування будь-якої послідовності двійкових цифр завадостійким кодом – умовно, не реально, не фізично – групи розрядів початкового числа розглядаються як деякі лишки, то такий код одержав найменування коду умовних лишків.

Слід звернути увагу на те, що при кодуванні ЛУ-кодом початкова послідовність не міняється, до неї тільки приформовуються додаткові, обчислені за окремими правилами, контрольні символи.

Таким чином ЛУ-код дозволяє знаходити і виправляти b-розрядні пакети спотворень, згруповані в межах будь-якої з n груп і вимагає при цьому надмірність біля: $r \approx 2b+1$ розрядів (оскільки $p_k \approx 2p_n p_{n-1}$, $r=[\log_2 p_k]+1$). У конкретних випадках ця надмірність може відхилятися в ту або іншу сторону, що залежить також від алгоритмів кодування-декодування.

Оскільки в основі ЛУ-коду лежать властивості СЛК, то в цьому коді принципово можуть бути використані відомі алгоритми кодування-декодування. В основі цих

алгоритмів лежить той факт, що будь-яке спотворення в одній з груп розрядів αі переводить початкове число з робочого діапазону $[0, P = \prod_{i=1}^{n} p_i)$ в діапазон $[P, R)$, де $R = p_k \cdot P$, тобто приводить до збільшенню початкового числа $A < P$ на деяку величину $l_i \cdot R_i$. Тут l_i і $R_i = \frac{R}{p_i}$ – цілі числа. Дійсно, якщо вихідне число:

$$A = \alpha_1, \alpha_2, ..., \alpha_i, ..., \alpha_n, \alpha_k$$

є спотвореним по основі p_i і має вид:

$$\widetilde{A} = \alpha_1, \alpha_2, ..., \widetilde{\alpha}_i, ..., \alpha_n, \alpha_k,$$

де

$$\widetilde{\alpha}_i = \{\alpha_i + \Delta\alpha_i\} (\text{mod } p_i),$$

то це є еквівалентним наступному перетворенню:

$$\widetilde{A} = (\alpha_1, \alpha_2, ..., \alpha_i, ..., \alpha_n, \alpha_k) + +(0,0,..., \Delta\alpha_i, ...,0,0) =$$
$$= (\alpha_1, \alpha_2, ..., \{\alpha_i + \Delta\alpha_i\} (\text{mod} p_i), ..., \alpha_n, \alpha_k).$$

При цьому величина спотворення перевищує величину робочого діапазону Р:

$$\Delta A = (0,0,..., \Delta\alpha_i, ...,0,0) > P,$$

оскільки тільки число виду:

$$\Delta A = l_i \cdot R_i = l_i \cdot \frac{R}{p_i}$$

має всі лишки, окрім лишка по основі p_i такими, що дорівнюють нулю. Але $\Delta A = l_i \cdot R_i > P = \frac{P}{p_k}$ тобто, навіть при $l_i = 1$, величина $\frac{R}{p_i} > \frac{R}{p_k}$ по тій причині, що $p_k > p_i$.

Відтак, сума $\widetilde{A} = A + \Delta A > P$, тобто спотворене число вийшло за межі робочого діапазону Р і попало в діапазон (P, R).

Відомі алгоритми кодування-декодування якраз і використовують цей факт.

Застосування запропонованих узагальнених кодів дозволяє забезпечити виявлення та виправлення спотворень в b-розрядних узагальнених символах в кожному із базових кодових слів.

Застосування таких кодів дозволить розв’язати сформульовану проблему щодо надійного забезпечення цілісності інформаційних об’єктів в умовах впливу пакетів помилок значної тривалості.

ЛІТЕРАТУРА

1. *Юдін О. К., Конахович Г. Ф., Корченко О. Г.* Захист інформації в мережах передачі даних: Підручник. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714 с., іл.

2. *Юдін О. К.* Кодування в інформаційно-комунікаційних мережах: Монографія. – К.: НАУ, 2007. –308 с.

3. *Bernard Sklar Digital communications* // Prentice Hall PTR, 2001 – 1099 p.