3. *Каменева І.П.* База даних еколого-енергетичного моніторингу: проектування та створення / *І.П. Каменева, В.О. Артемчук* // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2009. – № 50. – С. 66-72.
4. *Яцишин А.В.* Формування вибірки з бази даних еколого-енергетичного моніторингу / *А.В. Яцишин, В.О. Артемчук* // Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту : Матеріали Міжнародної наукової конференції, 18-22 травня 2009 р. - Херсон: ХНТУ, 2009. – Т.2. – Ч.2. – С. 114–117.

Поступила 10.03.2010р.

УДК 681.3

С.В. Василенко

МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ ІЗ ЗАСТОСУВАННЯМ УЗАГАЛЬНЕНОГО ЗАВАДОСТІЙКОГО КОДУ УМОВНИХ ЛИШКІВ

Summary: Explored possibilities of the use in the networks of telecommunication of model of providing of integrity of information holding object on the base of the generalized antigambling code of conditional tailings. In the article of such realizable analysis of his possibilities.

Вступ

Відповідно до термінології нормативних документів Державної служби спеціальних телекомунікаційних систем і захисту інформації України [1] під цілісністю інформації розуміється її властивість, яка полягає у тому, що інформація не може бути модифікована неавторизованим користувачем або процесом. Іншими словами, під цілісністю інформації розуміється відсутність в ній будь-яких викривлень (модифікацій), які не були санкціоновані її власником, не залежно від причин або джерел виникнення таких викривлень.

Викривлення інформації, тобто порушення її цілісності, можливі на будь-якому етапі її циркуляції у обчислювальних мережах: при зберіганні, передачі або обробці. Причини таких викривлень можуть бути випадковими або навмисними. У свою чергу, випадкові викривлення можуть бути як природними, пов'язаними з дією природних чинників, так і штучними. Випадкові штучні викривлення пов'язані з діяльністю людей − з випадковими помилками персоналу. Навмисні викривлення завжди пов'язані з умисними діями порушників. І ті, і інші дії мають своїм наслідком викривлення того або іншого числа символів в цифровому представленні інформації, незалежно від використовуваної системи числення або форми

представлення інформації і, в цьому значенні, є загрозами функціональним властивостям захищеності інформаційних ресурсів – їх цілісності і доступності. Надалі розглядається модель забезпечення цілісності інформаційних об'єктів в умовах природних впливів із застосуванням одного із узагальнених завадостійких кодів – коду умовних лишків.

Постановка задачі

Для забезпечення контролю та поновлення цілісності інформаційних об'єктів, включаючи і відновлення зруйнованої інформації, до складу інформації, яка захищається, включають надмірну інформацію – ознаку цілісності або контрольну ознаку (залежно від прийнятої в задачах контролю цілісності або завадостійкого кодування термінології) − своєрідний образ, відображення цієї інформації, процедура формування якого відома, і який з дуже високою вірогідністю відповідає інформації, що захищається.

При цьому моделі забезпечення цілісності істотно залежать від умов їх застосування, а саме від впливу випадкових (природних) або штучних (зловмисних) викривлень.

Серед основних моделей забезпечення цілісності інформації в умовах природних дій (проблема завадостійкості) слід виділяти:

1. Збільшення співвідношення сигнал/завада за рахунок підвищення енергетики сигналу, або за рахунок зниження рівня завад (шумів);

2. Забезпечення хоча б задовільної узгодженості смуги пропускання П каналу із спектром сигналу;

3. Застосування мажоритарних (групових) методів захисту;

4. Застосування різного роду завадостійких кодів з виявленням помилок в прийнятій (зчитаній) інформації;

5. Застосування різного роду завадостійких корегуючих кодів (ЗКК), які дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засобів виявлення і усунення викривлень.

Одним із класів таких кодів є узагальнені завадостійкі коди, зокрема код умовних лишків.

Узагальнені завадостійкі коди. Код умовних лишків

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

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

$$\underbrace{I_1 \ldots I_b}_{1\text{ – й УС}},\ \underbrace{I_{b+1} \ldots I_{2b}}_{2\text{ – й УС}}\ \ldots\ \underbrace{I_{m-b+1} \ldots I_m}_{n\text{ – й УС}}.$$

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 (лишків умовних код, ЛУ – код). Теоретичною основою ЛУ – коду є теорія лишкових класів. З теорії лишкових класів [2] 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 i = 1, 2, …, n, n – кількість таких основ. Вибір величини n здійснюється з умови, яка викладена нижче. Тоді

$$A = \alpha_1, \alpha_2, \ldots, \alpha_n, \qquad (1)$$

де $\alpha = A - [A/p_i]\cdot p_i$, а позначка $[A/p_i]$ означає операцію розрахунку цілої частини від дробового числа A/p_i. При цьому між числом А і його уявленням (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 викривлень. Відомо, що якщо ввести ще одну, контрольну, основу $p_к$, то уявлення А в розширеному діапазоні $R = P\cdot p_к$, у вигляді

$$A = \alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_k, \qquad (2)$$

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

Такий код має принаймні 2 недоліки. Перший з них пов’язаний з необхідністю роботи з числами в системі числення в залишкових класах, а другий – з тим, що можливі викривлення знаходяться і виправляються (викривлений символ поновлюється) тільки в тому випадку, якщо викривлений лише один з символів αi, тобто викривлення повинні бути фіксованими в межах однієї з груп розрядів.

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 і – ї групи (пакету) 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 рі. 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. Хай 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 αі 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 основами рі (i = 1, 2,...). Якщо розширити систему основ на контрольну p_k і для одержаного набору умовних лишків α_i (i = 1, 2,...) розрахувати умовний лишок α_k, то на одержане умовне число

$$A = \alpha_1, \alpha_2, \ldots, \alpha_{n1}, \alpha_к \qquad (3)$$

розповсюджується можливості СЛК по виявленню і виправленню викривлень, тобто одержаний код (3) має всі властивості коду (2), але останній код може бути отриманим для будь-якої двійкової послідовності, а не тільки по відношенню до 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 викривлень, згруповані в межах будь-якої з n груп і вимагає при цьому надмірність біля

$$r \approx 2b + 1$$

розрядів (оскільки $p_k \approx 2 p_n p_{n-1}$, $r = [\log_2 p_k] + 1$). В 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 викривлення в одній з груп розрядів αi 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 $R_i = R/p_i$ – цілі числа. Дійсно, якщо вихідне число

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

є викривленим по основі p_i і має вид

$$\widetilde{A} = \alpha_1, \alpha_2, \ldots, \widetilde{\alpha}_i, \ldots, \alpha_n, \alpha_к$$

де

$$\widetilde{\alpha}_i = \{\alpha_i + \Delta\alpha_i\} \pmod{p_i},$$

то це є еквівалентним наступному перетворенню

$$\widetilde{A} = (\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \alpha_k) + (0, 0, \ldots, \Delta\alpha_i, \ldots, 0, 0) =$$
$$= (\alpha_1, \alpha_2, \ldots, \{\alpha_i + \Delta\alpha_i\} \pmod{p_i}, \ldots, \alpha_{n1}, \alpha_k).$$

При цьому величина викривлення перевищує величину робочого діапазону P:

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

оскільки тільки число виду

$$\Delta A = l_i \cdot R_i = l_i \cdot R/p_i$$

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

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

Відомі алгоритми кодування-декодування як раз і використовують цей факт.

Висновки

1. Застосування запропонованих узагальнених кодів дозволяє забезпечити виявлення та виправлення викривлень в b − розрядних узагальнених символах в кожному із базових кодових слів.

2. Застосування таких кодів, на погляд автора, дозволить розв'язати сформульовану проблему щодо надійного забезпечення цілісності інформаційних об'єктів в умовах впливу пакетів викривлень значної тривалості.

1. *НД ТЗІ 2.5-005-99* "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу".

2. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. // М.: Сов. радио, 1966. – 421 с.

Поступила 22.02.2010р.