УДК 004.056.5(045) **Василенко В.С., Чунарьов А.В., Чунарьова А.В.**

ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ КОДУВАННЯ ПРИ ЗАБЕЗПЕЧЕННІ ЦІЛІСНОСТІ ІНФОРМАЦІЇ В СУЧАСНИХ ІКСМ

У статті проведено аналіз існуючих методів завадостійкого канального кодування захищених інформаційних мереж. Визначено кількісні оцінки ефективності використання коду умовних лишків з умови підвищення цілісність та достовірність інформації, яка зберігається, передається та оброблюється в сучасних інформаційних мережах.

Показано, що при використанні коду умовних лишків відбувається подальше повне усунення спотворень у інформаційному повідомленні з умов появи багатократних помилок.

Ключові слова: інформаційна безпека, завада, завадостійке кодування, інформаційний потік, цілісність.

Актуальність. На сьогодні процеси накопичення, зберігання і передачі інформації в інформаційно-комунікаційних системах та мережах (ІКСМ) протікають в умовах впливу як навмисних, та випадкових завад. Ці завади природного або штучного характеру здатні спотворити збережені і оброблювані дані, тобто порушити базові властивості інформації, а саме конфіденційність, цілісність та доступність.

У зв'язку з цим серед методів і засобів боротьби з загрозами порушення базових властивостей інформації особливе місце займає технологія завадостійкого кодування. Завадостійке кодування виконується з метою захисту інформації від випадкових та навмисних завад при передачі та зберіганні інформації в сучасних ІКСМ.

Для вирішення проблем передачі та захисту інформації в реальних системах зв'язку необхідне комплексне використання різних методів і засобів і тому застосування завадостійкого кодування допомагає ефективно використовувати канали зв'язку для надійного захисту переданої та збереженої інформації.

Постановка задачі. Збільшення швидкості передачі даних в каналі зв’язку тягне за собою зростання кількості випадкових та навмисних завад, спрямованих на спотворення інформації, яка зберігається, передається та оброблюється в сучасних інформаційних мережах. Це обумовлює актуальність розробки та використання нових методів, що дозволяють виявляти і коригувати подібні завади.

У цих умовах особливої уваги заслуговують завадостійкі коди, які, на відміну від криптографічного шифрування і стиснення, дозволяють ефективно боротися з випадковими та навмисними спотвореннями в каналі.

Завадостійкому кодуванню відводиться два основних завдання:

– підвищення ефективності та надійності захищених інформаційних систем та мереж;
– підвищення рівня захищеності цих систем та мереж.

Використання методів завадостійкого кодування інформації для досягнення інформаційної надійності та захищеності ІКСМ дозволяє здійснювати функції контролю передачі та зберігання інформації і забезпечує коректність цих процесів, а також забезпечує захист від несанкціонований дій і спотворень.

У зв'язку з цим завадостійке кодування обов'язково передбачає подальше відновлення та ідентифікацію інформації в первинний вигляд, придатний для її використання в процесах обробки і прийняття управлінських якісних рішень. Безпомилкове відновлення зменшить ймовірність появи помилок при прийняття рішень.

Можна навести інші переваги необхідності використання завадостійкого кодування в ІКСМ: надійна обробка і зберігання інформації, боротьба з групуванням помилок у захищених системах та мережах, захист інформації при передачі відкритих ключів і т. п.

Метою даної статті є проведення порівняльного аналізу існуючих методів завадостійкого канального кодування інформаційних потоків захищених ІКСМ.

Порівняльний аналіз сучасних методів завадостійкого кодування.

Сучасні інформаційні мережі широко використовують існуючі надлишкові коди з виявленням помилок (вони лише виявляють помилку) та коди з коригуванням (ці коди виявляють місце помилки і виправляють її).

Для різних типів завад в каналі зв'язку існують різні по своїй структурі і надмірності конструкції − завадостійкі коди.

Зазвичай надмірність коду знаходиться в межах 10…50%, або трохи більше. Широко використовуються: ***блочні коди*** *– для швидкого виявлення помилок та* ***згорткові коди*** *– для виправлення одиночних помилок*. Найбільш поширеними серед блочних кодів є коди з перевіркою на парність, матричні коди, коди Хеммінга, циклічні коди (наприклад, коди Боуза-Чоудхурі-Хоквингема та Ріда-Соломона).

Також існує клас лишкових кодів, серед яких є код умовних лишків (ЛУ-код), лишково-Хемінговий код (ЛХ–код) та лишкові-матричний код (ЛМ−код) [1,2,5]. Класифікація сучасних методів завадостійкого кодування наведена на рис.1. Також сучасні завадостійкі коди класифікують на узагальнені та двійкові.

Двійкові коди – це коди, які призначені для виявлення (виявлення і виправлення) однократних помилок. Під ***узагальненими*** розумітимемо коди, призначені для виявлення (виявлення і виправлення) пакетних спотворень (багатократних помилок) з кратністю b, в яких використовуються алгоритми кодування і декодування, аналогічні відповідним алгоритмам двійкових кодів, але по відношенню до узагальненого b − розрядного символу.

Операції над узагальненими символами виконуються до деякому модулю, тобто шукається лишок або найменший залишок від розподілу результату операції на деякий модуль. Це дало можливість для відмінності відповідних узагальнених кодів від двійкових ввести в їх назву слово "лишок", тобто говорити про код умовних лишків, лишково - Хеммінгові, лишково - матричні, лишково - рекурентні (ЛР) коди.

Слід зазначити, що лишкові - циклічні коди відомі під назвою кодів Ріда - Соломона - на ім'я авторів цих кодів [3, 4]. На цей час існуючі види завадостійкого кодування відрізняються один від одного наступними характеристиками: відносною швидкістю, надмірністю, виявляючою та корегуючою здатністю, структурою, функціональним призначенням, енергетичною ефективністю, тощо.

При виборі та використанні обраного типу завадостійкого кодування для підвищення достовірності та цілісності інформаційних потоків ІКСМ потрібно врахувати: характер розподілу помилок в каналі зв'язку; допустиму ймовірність появи помилок в кодовій комбінації; складність алгоритмів кодування.

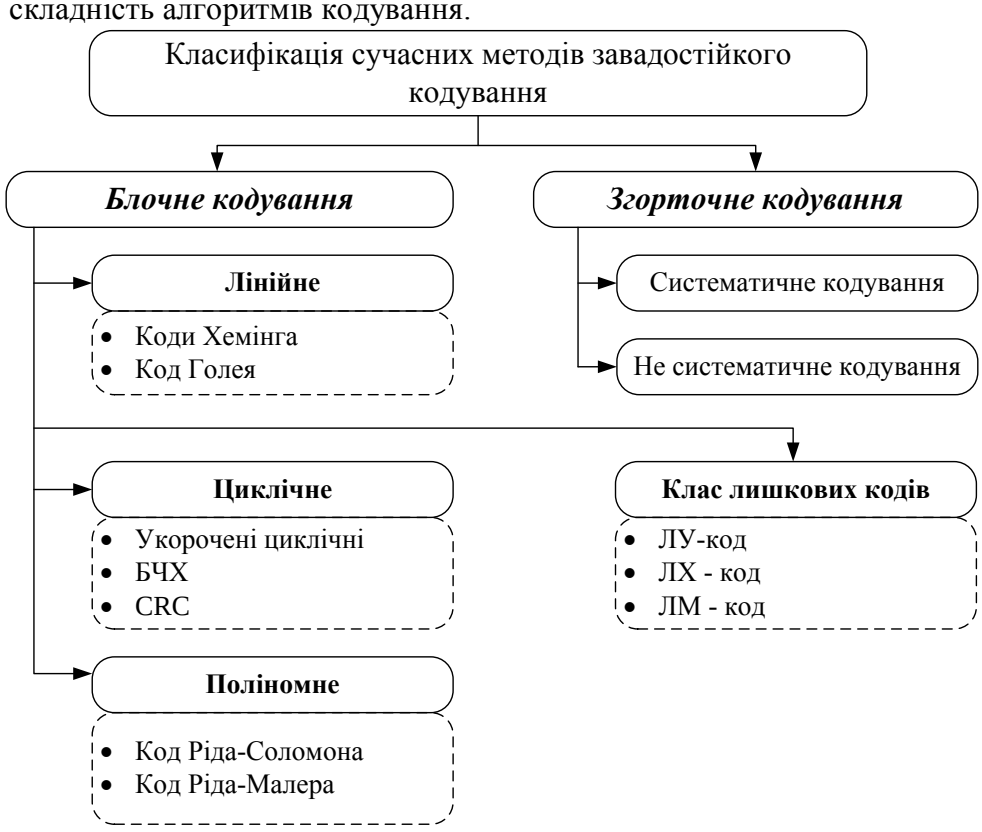

Рис. 1. Класифікація завадостійкого кодування

Одним з основних факторів вибору коду є характер розподілу помилок в каналі зв'язку, який визначає корегуючу здатність такого коду. Помилки які виникають в реальних каналах зв'язку є залежними та мають тенденцію до групування (пакетування), тобто виникають багатократні помилки. Однак, більшість сучасних методів завадостійкого кодування направленні на виявлення та коригування тільки однократних помилок та повністю втрачають свій сенс при виникнення багатократних пакетних помилок.

Основні характеристики методів завадостійкого кодування.

Далі для проведення оцінки ефективності існуючих методів кодування потрібно визначити їх характеристики, за якими вони будуть порівняні. До основних характеристик можна віднести наступні [1]:

1. *Значність коду,* або *довжина базового кодового слова*, яка включає інформаційні символи (m) і перевірочні, або контрольні, біти (k). Звичайно значність коду n є сума

$$n = m + k . \tag{1.1}$$

2. *Відносна швидкість коду* − R є відношенням числа інформаційних символів в кодовій комбінації m до значності коду n:

$$R = m/n . \tag{1.2}$$

3. *Надмірність коду* K є відношенням числа контрольних символів в кодовій комбінації k до значності коду n та показує корегуючу здатність коду:

$$K = 1 - m/n = 1 - R . \tag{1.3}$$

4. *Ймовірність появи символьних помилок в каналі звязку з кодуванням* Pc:

$$Pc = Q\left(\sqrt{\frac{R \cdot E_c}{N_0}}\right), \tag{1.4}$$

де $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp\left(\frac{-u^2}{2}\right) du$ − гаусів інтеграл помилок, $\frac{E_c}{N_0}$ – відношення енергії кодованого біту до спектральної щільності потужності шуму в каналі зв'язку; R − відносна швидкість коду.

Далі наведемо оцінку ефективності використання сучасних методів завадостійкого кодування з метою забезпечення цілісності інформації.

Для порівняння були вибрані найбільш поширені методи завадостійкого кодування, які використовуються для забезпечення цілісності при передачі та збереженні інформації (табл. 1-2).

У таблиці зведені методи блочного кодування (код Хеммінга, CRC-32, CRC-64 та матричний код) з метою виявлення або виправлення однократних помилок t=1 та клас лишкових кодів на основі виявлення та виправлення пакетів помилок t=8 [3, 4]. Проведемо порівняльний аналіз коду умовних лишків з існуючими методами завадостійкого кодування/декодування інформаційних потоків та покажемо його ефективність застосування з точки зору забезпечення цілісності інформаційного потоку даних. Визначимо оцінку ефективності використання коду умовних лишків з умов забезпечення достовірності і цілісності кодових конструкцій та підвищення захисту інформації в сучасних ІКСМ.

Для оцінки якості коду умовних лишків була розрахована ймовірність появи символьних помилок кратністю t від заданого співвідношення сигнал/шум в каналі зв'язку (табл. 1.2, рис. 2-5).

З отриманих аналітичних та графічних залежностей, можна зробити наступні висновки:

по-перше, використання коду умовних лишків в задачах забезпечення цілісності дозволяє зменшити кількісні значення ймовірностей появи символьних помилок знизилася від 1,02 до 2,82 разів для коду умовних лишків в порівнянні з відомими методами;

по-друге, при використання коду умовних лишків надлишковість в залежності від використаного завадостійкого коду зменшилася від 2 до 13,4 разів, що дозволило зменшити складність реалізації коду;

по-третє, відносна швидкість коду при використанні коду умовних лишків збільшилася від 1,01 до 1,11 разів.

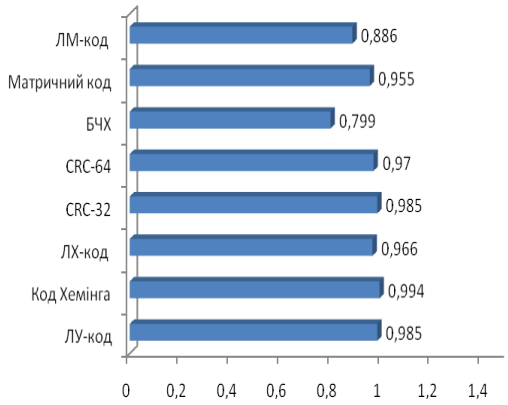

Рис. 2. Відносна швидкість завадостійкого коду

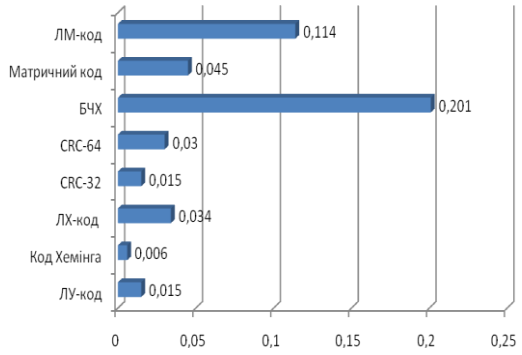

Рис. 3. Надлишковість коду завадостійкого коду

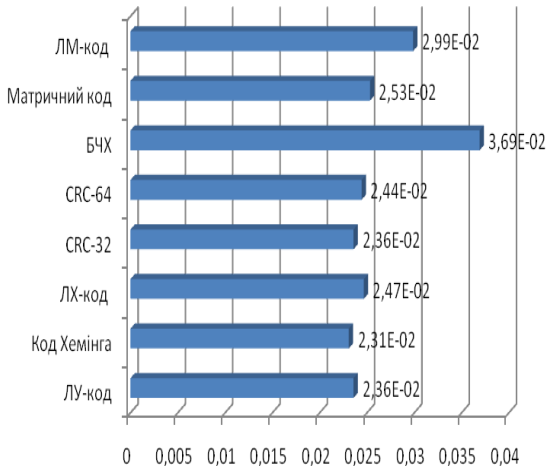

Рис. 4. Ймовірність появи символьних помилок t в каналі зв'язку з кодуванням, порівняння сучасних методів (при $E_c / N_0 = 2 дБ$)

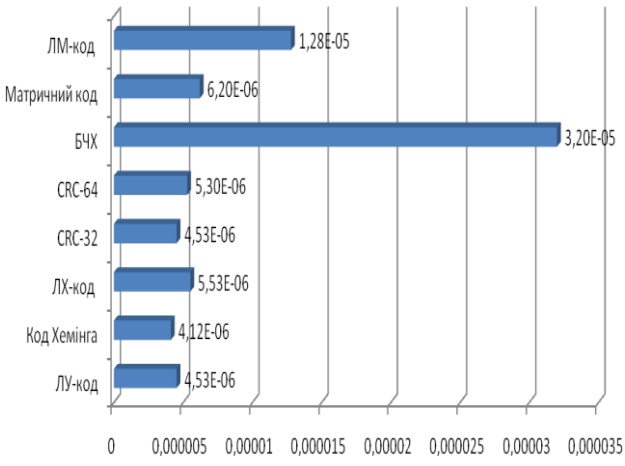

Рис. 5. Ймовірність появи символьних помилок t в каналі зв'язку з кодуванням, порівняння сучасних методів (при $E_c / N_0 = 10 дБ$)

Таблиця 1

Характеристики методів завадостійкого кодування

Назва коду	**Кількість інформаційних біт,** *m*	**Кількість контрольних біт,** *k*	**Значність коду,** *n*	**Корегуюча здатність,** *t*
ЛУ-код	2048	32	2080	8
Код Хемінга	2048	12	2060	1
ЛХ-код	2048	72	2120	8
CRC-32	2048	32	2080	1
CRC-64	2048	64	2112	1
БЧХ	255	64	319	8
Матричний код	2048	97	2145	1
ЛМ-код	2048	264	2312	8

Висновки. У статті проведено порівняльний аналіз існуючих методів завадостійкого канального кодування інформаційних потоків ІКСМ. Проведені дослідження показали, що застосування коду умовних лишків дозволяє підвищити цілісність та достовірність інформації, яка зберігається, передається та оброблюється в сучасних інформаційних мережах.

Таблиця 2

Імовірності появи символьних помилок при використанні методів завадостійкого кодування

Назва коду	**Відносна швидкість,** $R=m/n$	**Надлишковість коду,** $K=k/n$	Pc, **при** $E_c / N_0 = 2дБ$	Pc, **при** $E_c / N_0 = 10дБ$
ЛУ-код	0,985	0,015	2,35754e-2	4,53007e-6
Код Хемінга	0,994	0,006	2,30765e-2	4,12292e-6
ЛХ-код	0,966	0,034	2,46663e-2	5,52712e-6
CRC-32	0,985	0,015	2,35754e-2	4,53007e-6
CRC-64	0.97	0,03	2,44323e-2	5,30035e-6
БЧХ	0,799	0,201	3,69093e-2	3,20076e-5
Матричний код	0,955	0,045	2,53221e-2	6,20224e-6
ЛМ-код	0,886	0,114	2,98806e-2	1,27961e-5

Таким чином, показано, що при використанні коду умовних лишків відбувається зменшення ймовірностей появи символьних помилок та подальше повне усунення спотворень у інформаційному повідомленні з умов появи багатократних помилок, що підвищує ефективність та надійність функціонування ІКСМ з умов збільшення вірогідності інформаційного потоку даних, без втрат якості. Тобто, відбувається зменшення ймовірність появи символьних помилок та повне усунення спотворень у інформаційному повідомленні.

Використання даного коду дозволяє виявляти та виправляти багатократні помилки та усувати спотворення. Також, відбувається підвищення швидкості передачі даних, збільшення вірогідного потоку даних, економія смуги частот ІКСМ.

ЛІТЕРАТУРА

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Пер. с англ. – М.: Изд. дом Вильямс, 2004. – 1104 с.

2. Юдін О.К. Кодування в інформаційно-комунікаційних мережах – Монографія. К.: Книжкове видавництво НАУ, 2007. – 302 с.

3. Василенко В.С. Узагальнені завадостійкі коди в задачах забезпечення цілісності інформаційних об’єктів в умовах природних впливів / В.С. Василенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. –2006. – Вип. 2 (13) – С. 144 −159.

4. Пат. 67988 Україна, МПК H03M 13/00 Спосіб забезпечення цілісності інформації на базі завадостійкого коду умовних лишків/ Василенко В.С., Василенко М.Ю., Чунарьов А.В.; заявник та патентовласник Нац. авіац. ун-т. – u201110207; заявл. 19.08.2011; опубл.12.03.2012, Бюл. №. 5 – 4 с.

5. Чунарьов А.В. Забезпечення цілісності інформаційних ресурсів на базі методів завадостійкого кодування/ А.В.Чунарьов, М.Ю.Василенко // Наукоємні технології: наук.-техн. конф. студентів та молодих учених (Київ, 11–12 листопада 2011 р.) – К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», 2011. – С.11.

Надійшла: 27.07.2012 р.

Рецензент: д.т.н., професор Юдін О.К.

УДК 004.056.55:004.312.2

Рудницький В.М., Бабенко В.Г., Рудницький С.В.

МЕТОД СИНТЕЗУ МАТРИЧНИХ МОДЕЛЕЙ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕКОДУВАННЯ ІНФОРМАЦІЇ

У роботі запропонований математичний апарат, який покладений в основу розробки методу синтезу матричних моделей операцій криптографічного перекодування інформації на основі заданих вхідної та вихідної операцій криптографічного кодування.

Ключові слова: матрична модель, операція криптографічного перекодування, матриця перекодування.

Постановка проблеми у загальному вигляді та її зв'язок із важливими практичними завданнями. У даний час основними засобами захисту інформації в системах і мережах є криптографічні засоби, що реалізують різноманітні методи шифрування. Але