УДК 519.15..621.372

О. Різник, В. Ковалик, О. Повшук
Національний університет “Львівська політехніка”,
кафедра інформаційних технологій видавничої справи

ВІДНОВЛЕННЯ ПОШКОДЖЕНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ЗАВАДОСТІЙКИХ КОДІВ

Метою роботи є дослідження завадостійких кодів на основі ідеальних кільцевих відношень для відновлення пошкодженої інформації. Для запобігання втратам цифрових даних створено ефективний завадостійкий код на основі ідеальних кільцевих в’язанок для захисту та відновлення інформації, який забезпечує можливість виправлення до 25 % помилок у кодовому слові. Розроблений програмний продукт, який моделює роботу завадостійкого коду на основі ідеальних кільцевих в’язанок.

Ключові слова: ідеальна кільцева в’язанка, завадостійкий код, код БЧХ, код Хеммінга.

The purpose of work is research of error controlled codes on the basis of ideal ring bundles for proceeding in the damaged information. For prevention of losses of digital data an effective error controlled code is created on the basis of ideal ring bundles for defence and proceeding in information, which provides possibility of correction to the 25% errors in a code word. Worked out software product which designs work of error controlled code on the basis of ideal circular bundles.

Key words: idea ring bundle, error controlled code, BCH code, Hamming code.

Вступ

Актуальність питання захисту даних сьогодні визначається такими основними факторами:

– розширенням сфери використання інформаційних технологій, різноманіттям і межами поширення інформації, високими темпами збільшення кількості техніки;

– підвищенням рівня віри в автоматизовані системи управління і опрацювання інформації;

– залученням до процесу обробки інформації все більшої кількості людей та підприємств, різким зростанням їхніх інформаційних потреб, наявністю інтенсивного руху інформації між учасниками процесу;

– концентрацією великих обсягів інформації різного призначення, яка записана на електронних носіях;

– ставленням до інформації як до товару, переходом до ринкових відносин у сфері надання інформаційних послуг з конкуренцією і промисловим шпигунством;

– різноманіттям видів загроз і виникненням нових можливих каналів несанкціонованого доступу до інформації;

– зростанням кількості кваліфікованих користувачів комп’ютерів і можливостей їхніх програмно-математичних дій, небажаних для системи опрацювання інформації;

– розвитком ринкових відносин (у сфері розроблення, поставки, обслуговування обчислювальної техніки, розроблення програмних засобів, зокрема засобів захисту інформації).

Постановка проблеми

Головною проблемою, яка розглядається в статті, є виникнення завад в інформації, яка утворилась через збільшення кількості користувачів комп’ютерної техніки, великий обсяг обороту інформації, підвищення цінності цифрової інформації та збільшення видів загроз.

Мета − знайти завадостійкий код, який би був простим у побудові та мав завадостійкі параметри, не гірші, ніж у загальновідомих кодів.

Вирішення проблеми

В основу побудови завадостійких кодів, як відомо, покладено принцип введення надлишковості, що дає змогу виявляти та виправляти помилки за рахунок накладення додаткових вимог до переданих сигналів з подальшою їх перевіркою. Серед великої різноманітності таких кодів особливе місце займають циклічні, широке застосування яких на практиці зумовлено високою ефективністю під час виявлення та виправлення помилок, а також порівняно простою реалізацією кодувальних і декодувальних пристроїв.

Як уже згадувалося вище, цей параметр пов'язаний з коректувальними властивостями коду. До них зараховують властивості виявляти помилки, виправляти помилки та виправляти помилки меншої кратності й виявляти помилки більшої кратності. В цьому контексті можна виділити такі моменти:

– що більша мінімальна кодова відстань коду, то краща його здатність виявляти помилки;

– потрібно розрізняти поняття "мінімальна кодова відстань для пари кодових комбінацій" і "мінімальна кодова відстань для коду".

Для запобігання втратам цифрових даних створено ефективний завадостійкий код на основі ідеальних кільцевих в'язанок (ІКВ) для захисту та відновлення інформації [2].

Ідеальна кільцева – це циклічна послідовність n чисел, на якій всі можливі кільцеві суми вичерпують R-разів значення чисел натурального ряду від 1 до $S_n = \frac{n(n-1)}{R} + 1$ (рис. 1) [1].

Рис. 1. Ідеальна кільцева в'язанка з параметрами $n = 4$ *та* $R = 1$

Опишемо побудову коду на основі ідеальних кільцевих в'язанок з параметрами $n = 4$ та $R = 2$, де 1 відповідає 1, 2 – відповідає послідовності 10, 3 – 100 і т.д. (рис. 2).

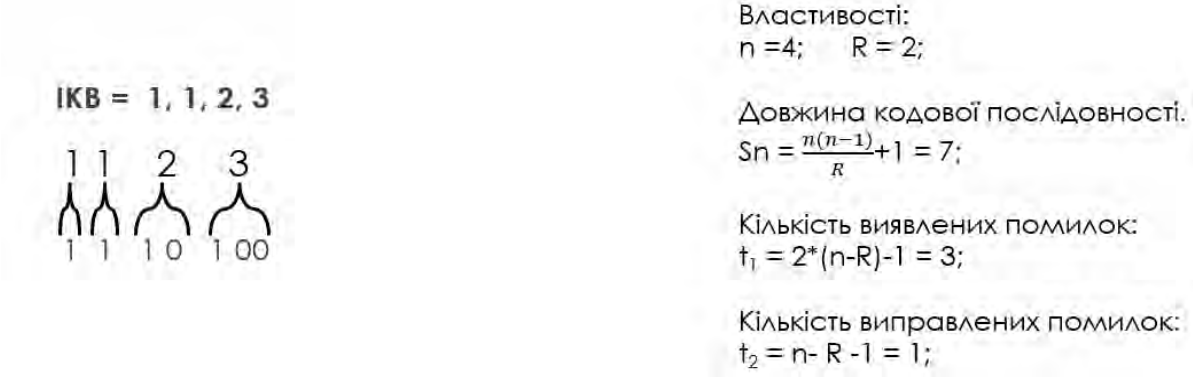


Рис. 2. Графічне представлення побудови коду на ІКВ з параметрами $n = 4$ *та* $R = 2$

Для оптимальних параметрів завадостійкого коду на основі ІКВ залежно від поставленої задачі дуже цінним є зв'язок між мінімальною кодовою відстанню та коректувальними властивостями коду щодо знаходження помилок (1) та їх виправлення (2):

$$t_d = d_{\min} - 1, \tag{1}$$

$$t_c = \frac{d_{\min} - 1}{2}. \tag{2}$$

Варто розуміти, що зі збільшенням мінімальної відстані, поряд зі зростанням коректувальних властивостей, ми збільшуємо надлишковість коду. Тому в цій ситуації оптимальний вибір коректувальних властивостей коду за формулою (3) є надзвичайно важливим.

$$d_{\min} = 2(n - R) \tag{3}$$

Розглянемо побудову кодувального алфавіту методом циклічного зсуву первинної послідовності, додавання інверсних послідовностей, послідовностей нулів та одиниць та біта перевірки на парність (рис. 3).

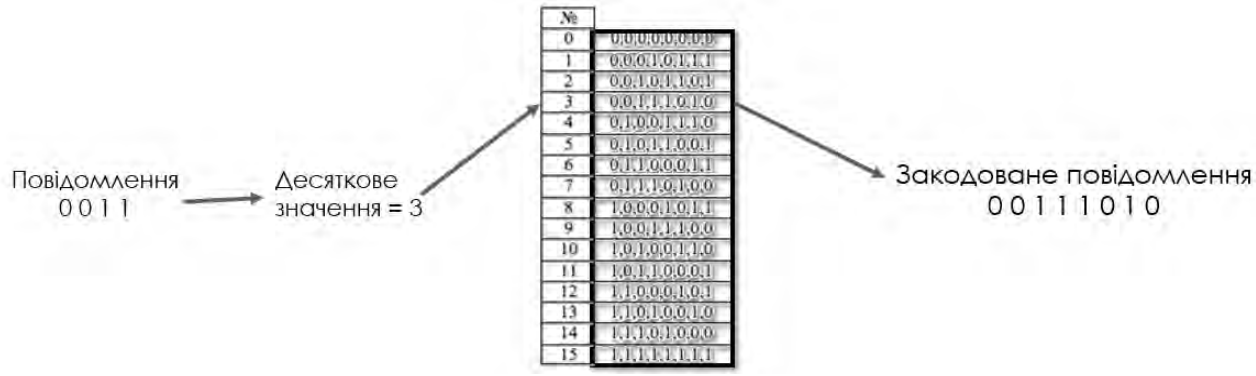


Рис. 3. Приклад кодування повідомлення на ІКВ з параметрами $n = 4$ *та* $R = 2$

Декодування та виправлення помилки у переданому повідомленні на ІКВ з параметрами $n = 4$ та $R = 2$ показано на рис. 4.

Порівнюємо вхідну закодовану послідовність (рис. 3) з кодувальним алфавітом. Найподібніша послідовність буде правильною.

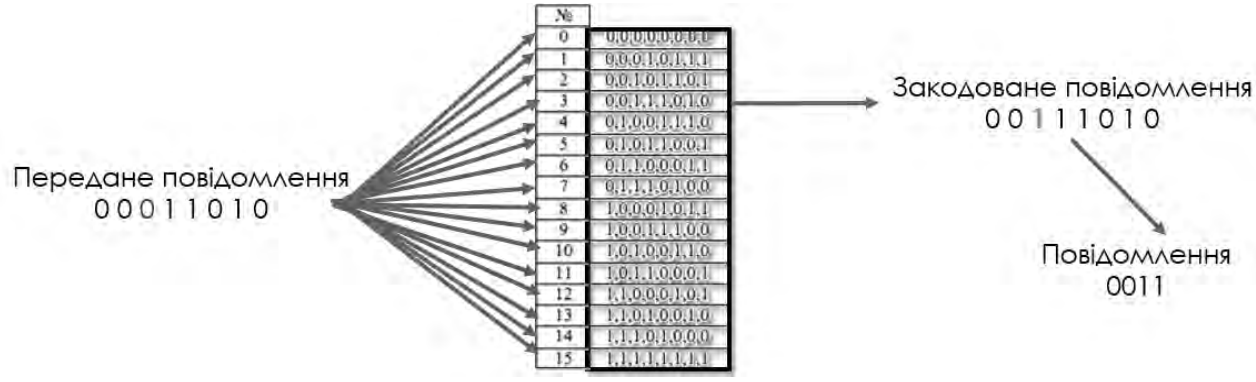
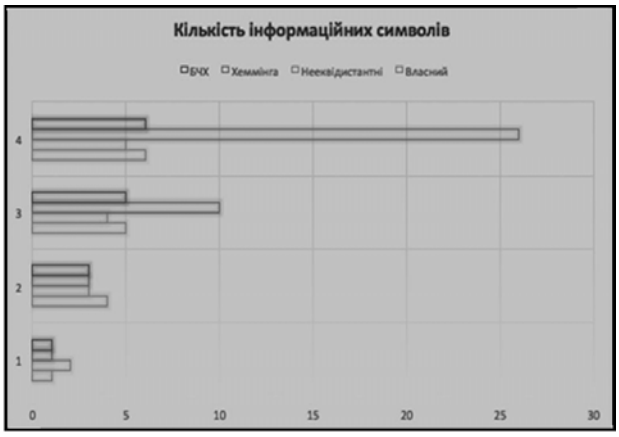


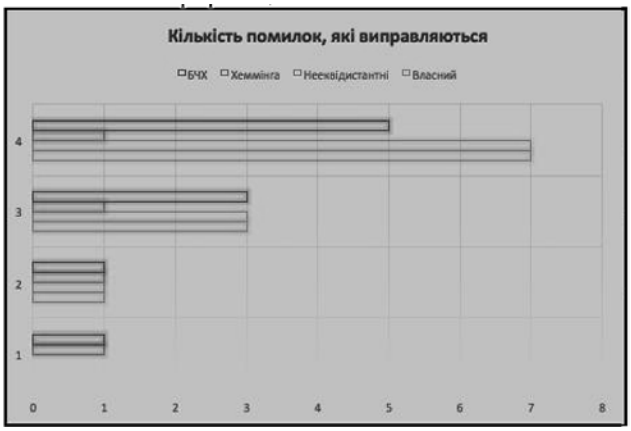
Рис. 4. Приклад декодування переданого повідомлення на ІКВ з параметрами $n = 4$ *та* $R = 2$

Порівняємо запропонований завадостійкий код із загальновідомими рішеннями щодо кількості інформаційних символів (рис. 5), кількості помилок, які виправляються (рис. 6), та потужності коду на основі залежності S_n та формул (1)–(3) [1, 2].



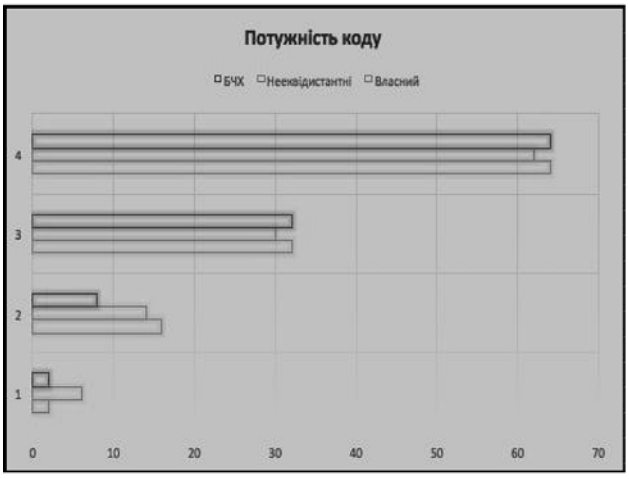
№	N	Ni_Власний	Ni_Нееквідистантний	Vi_Хеммінга	Vi_БЧХ
1	3	1	2	1	1
2	7	4	3	3	3
3	15	5	4	10	5
4	31	6	5	26	6

Рис. 5. Порівняння власного коду на ІКВ з кодами БЧХ, Хеммінга та нееквідистантним за кількістю інформаційних символів



№	N	t2_Власний	t2_Нееквідистантний	t2_Хеммінга	t2_БЧХ
1	3	0	1	1	1
2	7	1	1	1	1
3	15	3	2	1	3
4	31	7	2	1	5

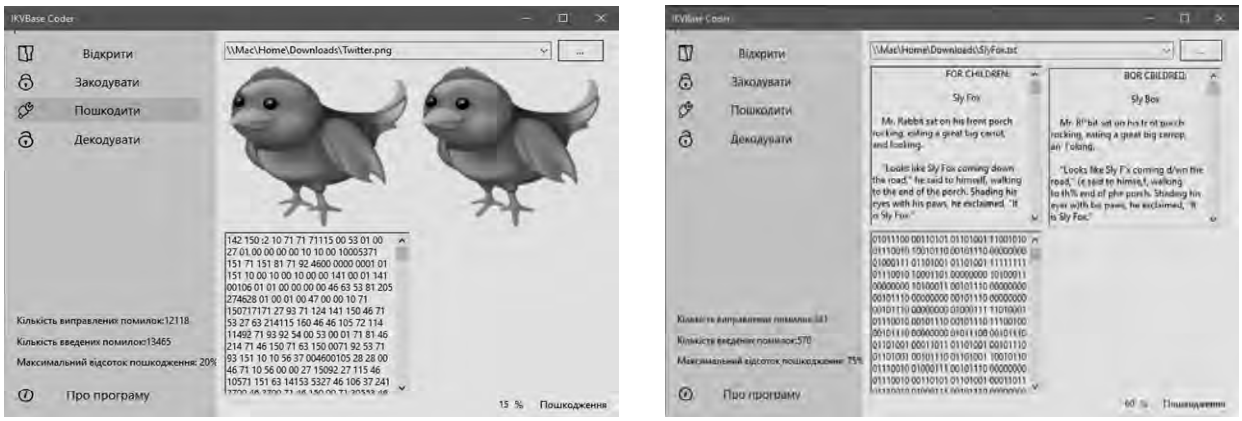
Рис. 6. Порівняння власного коду на ІКВ з кодами БЧХ, Хеммінга та нееквідистантним за кількістю помилок, які виправляються



№	N	P_Власний	P_Нееквідистантний	P_БЧХ
1	3	2	6	2
2	7	16	14	8
3	15	32	30	32
4	31	64	62	64

Рис. 7. Порівняння власного коду на ІКВ з кодами БЧХ, Хеммінга та нееквідистантним за потужністю коду

Розроблено програмний продукт, який моделює роботу завадостійкого коду на основі ІКВ. Загальний вигляд програми, якщо кількість введених помилок більша від кількості виправлених для графічного зображення та тексту, представлений відповідно на рис. 8, *а*, *б*.



а *б*

Рис. 8. Загальний вигляд програми, яка моделює роботу завадостійкого коду на основі ІКВ

Висновки

Розроблено модель завадостійких кодів на основі ідеальних кільцевих в’язанок, яка забезпечує можливість виправлення до 25 % помилок у кодовому слові, виправлено високу надлишковість порівняно з нееквідистантною кодовою послідовністю, що дає змогу конкурувати вже з відомими рішеннями кодів Хеммінга та БЧХ. Це уможливить її використання у багатьох сферах для збереження цілісності даних.

1. Різник В. В. Синтез оптимальних комбінаторних систем. – Львів, 1989. 2. Різник О. Я., Балич Б. І. Використання числових лінійок-в’язанок для кодування інформації // Комп’ютерні науки та інформаційні технології. – 2006. – С. 62–64.