МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ К. Д. УШИНСЬКОГО

Кафедра прикладної математики та інформатики

Ширшков О. К., Крапівна О. В.

ТЕОРІЯ ІНФОРМАЦІЇ ТА КОДУВАННЯ

Методичні вказівки та контрольні завдання до практичних занять студентів, вивчаючих дисципліни комп'ютерно - інформаційного циклу.

Одеса 2010

Методичні вказівки та контрольні завдання дисципліни "Теорія інформації та кодування" розроблені кандидатом технічних наук Ширшковим Олександром Костянтиновичем доцентом кафедри прикладної математики та інформатики ПНПУ ім. К. Д. Ушинського і ст. викладачем цієї ж кафедри Крапівною Ольгою Вікторівною.

Методичні вказівки та контрольні завдання дисципліни "Теорія інформації та кодування" розглянуто та схвалено кафедрою прикладної математики та інформатики ПНПУ ім. К. Д. Ушинського 01.02.2010 р., протокол №8.

Рецензенти:

- **зав. кафедрою прикладної, обчислювальної математики та систем автоматизованого проектування Одеської державної академії будівництва та архітектури, доктор фіз.-мат. наук, професор**

А. В. Плотніков .

- **доцент кафедри математичного аналізу ПНПУ ім. К.Д. Ушинського**

кандидат фіз.-мат. наук, доцент І. Ю. Дмитрієва.

Методичні вказівки та контрольні завдання дисципліни "Теорія інформації та кодування" рекомендовано до друку Вченою Радою ПНПУ ім. К. Д. Ушинського 25.02.2010 р. , протокол №_____.

Комп'ютерна верстка – ст. лаборант кафедри прикладної математики та інформатики ПНПУ ім. К. Д. Ушинського Швець Є.Д.

Зміст

1. Мета та задачі дисципліни

Мета дисципліни – ознайомити студентів з основними принципами теорії інформації і кодування, та засобами та ефективної передачі даних.

Задачами дисципліни є придбання студентами практичних навичок використання основних положень теорії інформації і кодування в процесі використання математичного, та програмного забезпечення, що повинно забезпечити уміння студентів:

- установлювати кількісну і якісну оцінку інформації;
- обчислювати інформаційні втрати, швидкість передачі інформації та пропускну здатність каналу зв’язку;
- використовувати засоби оптимального кодування для компресії даних;
- будувати системи захисту даних від несанкціонованого доступу;
- будувати коригуючи, завадостійкі коди;

Теорія інформації і кодування є розділом кібернетики, у якому математичними методами вивчаються способи виміру кількості інформації, методи кодування для ощадливого, стиснутого представлення повідомлень і надійної передачі повідомлень по каналах зв'язку із шумами. В основі математичного апарату теорії інформації і кодування лежать ймовірні та статистичні методи.

Актуальність теорії інформації і кодування, а також технічних проблем, зв'язаних з передачею, обробкою і збереженням інформації, росте пропорційно збільшенню обсягів інформації, що спостерігається у всіх областях науки і техніки. Важливими стають проблеми компресії даних, захисту від несанкціонованого доступу, та дії завад на каналах зв’язку. Відкриваються нові класи кодів, удосконалюються методи і пристрої кодування і декодування. Одночасно збільшується потреба у фахівцях, знайомих як з теорією інформації і кодування, так і з практичними питаннями, зв'язаними з передачею, обробкою, збереженням і захистом інформації.

Одна з основних задач теорії інформації — це максимальне використання потенційних можливостей локальних, корпоративних і глобальних комп'ютерних систем, шляхом спільної реалізації оптимального, завадостійкого та криптографічного кодування повідомлень.

2. Структура дискретного інформаційного каналу

Інформаційну систему передачі даних по каналі зв'язку можна представити у виді трьох укрупнених блоків: джерело повідомлень (ДП), лінія зв'язку (ЛЗ), приймач повідомлень (ПП).

Джерело виробляє повідомлення; кодери джерела перетворюють повідомлення в кодові слова, використовуючи методи оптимального, завадостійкого та криптографічного кодування. Модулятор перетворює бінарні коди в електричні сигнали.

Лінія зв'язку – це фізичне середовище у якому поширюються сигнали: провідні, кабельні, радіо та супутникові лінії.

Приймач – виконує зворотне перетворення: демодулятор перетворює електричні сигнали у бінарні коди, декодери виконують діагностику та корегування помилок, знімають стиснення, завадостійкий та криптографічний захист інформації.

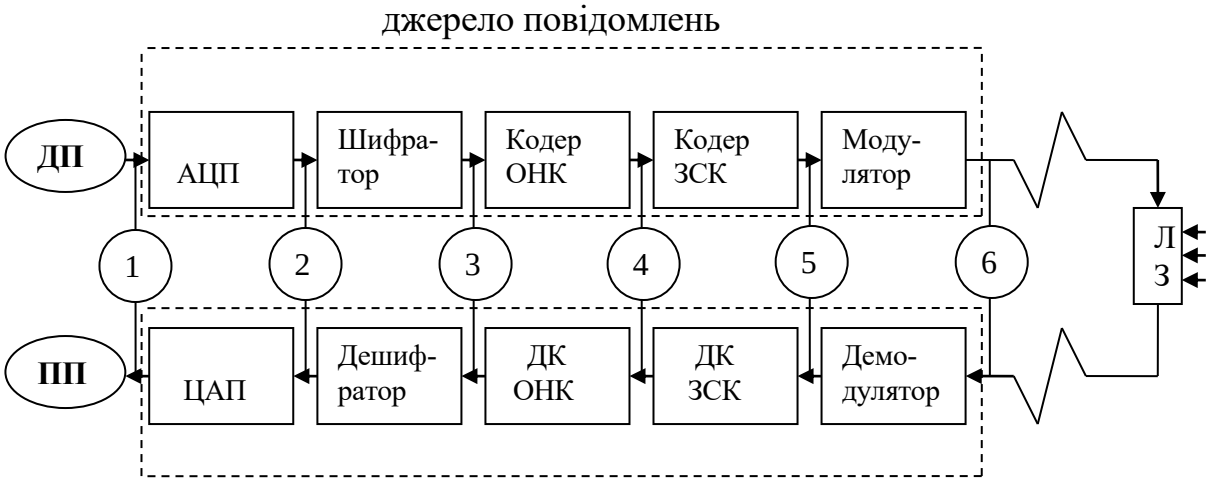


Рис. 1. Модель системи передачі дискретних повідомлень

На ідеальних каналах перешкоди відсутні, а на реальних каналах перешкоди обов'язково є. Джерело і приймач складається з апаратних і програмних блоків, що забезпечують ефективність дискретного каналу зв'язку.

Функції блоків:

АЦП (аналогово-цифрової перетворювач) - безперервна інформація перетвориться в дискретну.

Шифратор - встановлює криптографічний захист даних.

Кодер ОНК (оптимальне нерівномірне кодування) - стискає дані, компресія.

Кодер ЗСК (завадостійке кодування) - встановлює захист даних від перешкод.

Модулятор - перетворює цифрові дані в електричні сигнали.

Лінії зв'язку: дротяні, кабельні, радіо канали, супутникові канали.

Демодулятор - електричні сигнали перетворяться в цифрові дані.

ДК (декодер**) ЗСК** - виявляє наявність помилок в даних, обчислює адресу помилки і коректує її.

ДК ОНК - перетворює ОНК до рівномірного двійкового коду.

Дешифратор - знімає криптографічний захист.

ЦАП (цифро-аналоговий перетворювач**)** - цифрова інформація перетвориться в безперервну.

Модулятор і демодулятор конструктивно об’єднані в одному блоці – модем, а кодери і декодер об’єднуються у кодекс.

За структурою повідомлення поділяються на безперервні і дискретні. Дискретні повідомлення, як засіб передачі інформації, знайшли більш широке застосування. Можливість передачі безперервних повідомлень за допомогою дискретних сигналів була доведена академіком В.А. Котельниковим. Відповідно до теореми відліку бінарні дані цілком визначається сукупністю дискретних величин. Апроксимація з заданою точністю безперервних повідомлень дискретними даними називається *квантуванням*, а відрізок часу між двома сусідніми значеннями – *кроком квантування*. Абсолютне точне квантування неможливе, так само, як не можливо абсолютно точна передача думки. Який би багатим не був словниковий запас людини: думка – безперервна, словник – дискретний.

Дискретні дані в меншому ступені піддаються впливові перешкод комп'ютерних мереж, перекручування дискретного сигналу легше знайти і, головне, дискретні дані надійно та ефективно обробляються ЕОМ. Тому в даній дисципліні розглядаються дискретні повідомлення, та дискретні канали зв’язку.

3. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ І ПРИКЛАДИ РОЗВ’ЯЗАННЯ КОНТРОЛЬНИХ ЗАВДАНЬ

Практичні заняття виповнюються по індивідуальним вихідним даним для відпрацьовування питань контрольнихробіт.

3.1. Інформаційні та швидкісні характеристики дискретного каналу .

Центральною задачею теорії інформації, є визначення кількості інформації, інформаційних втрат, швидкісних характеристик, надійності та ефективності каналу зв’язку.

Інформаційний канал зв'язку вважається цілком заданим у трьох випадках:

1) надано безумовні імовірності джерела повідомлень $p(a_i)$ і канальна матриця з боку джерела виду $p(b_j/a_i)$;
2) Надано безумовні імовірності приймача повідомлень $p(b_j)$ і канальна матриця з боку приймача виду $p(a_i/b_j)$;
3) Надано канальну матрицю об'єднання виду $p(a_i;b_j)$.

Розташовуючи даними одного з трьох варіантів, можна обчислити всі інші інформаційні характеристики джерела, каналу зв'язку і приймача повідомлень.

Надійність, та ефективність каналу зв’язку визначають дві основні теореми К. Шеннона.

Теорема 1. «Про швидкість передачі» Визначає критичну швидкість передачі даних $R_{кр}$, залежну тільки від розподілу ймовірностей, при якій існує засіб передачі із швидкістю R близької до критичної ($R<R_{кр}$), при якій можливо відновлення початкового повідомлення (якщо швидкість $R>R_{кр}$, відновлення повідомлення неможливо). Критична швидкість дорівнює:

$$R_{кр} = \frac{C}{H(A)},$$

де H(A) - ентропія джерела, а C - пропускна здатність каналу.

Теорема 2. «Про кодування» Якщо продуктивність джерела *H'(A)* менше пропускної здатності каналу:

$$H'(A)<C,$$

то існує засіб кодування і декодуванні інформації при якій імовірність помилки може бути скільки завгодно мала та навпаки.

Розглянемо розрахунок інформаційних характеристик дискретного каналу на прикладі.

Задача. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку.

$$p(b_j / a_i) = \begin{Vmatrix} 0{,}98 & 0{,}01 & 0{,}01 \\ 0{,}10 & 0{,}75 & 0{,}15 \\ 0{,}20 & 0{,}30 & 0{,}50 \end{Vmatrix}.$$

Безумовні імовірності появи символів на виході джерела повідомлень дорівнює $p(a_1) = 0{,}7$; $p(a_2) = 0{,}2$; $p(a_3) = 0{,}1$. Тривалість передачі одного символу $\tau = 0{,}0002$ сек., передано повідомлення з 400 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Рішення

1. Кількість інформації $I(a_i)$ кожного символу a_1, a_2, a_3 дискретного повідомлення A :

$$I(a_i) = -\log p(a_i) \ (i=1,2,3), \text{ біт},$$

$$I(a_1) = -\log p(a_1) = -\log 0{,}7 = 0{,}5146, \text{ біт},$$
$$I(a_2) = -\log p(a_2) = -\log 0{,}2 = 2{,}3220, \text{ біт},$$
$$I(a_3) = -\log p(a_3) = -\log 0{,}1 = 3{,}3220, \text{ біт}.$$

2. Середня кількість інформації, передана одним символом визначає ентропія джерела повідомлень $H(A)$:

$$H(A) = -\sum_{i=1}^{3} p(a_i) \log p(a_i) = -(0{,}7 \log 0{,}7 + 0{,}2 \log 0{,}2 + 0{,}1 \log 0{,}1) = 1{,}1568 \text{ біт/символ}.$$

3. Максимальна ентропія джерела повідомлень $H_{max}(A)$

$$H_{max}(A) = \log N = \log 4 = 2 \text{ біт/символ},$$

де N-кількість символів у алфавіті повідомлення.

4. Інформаційні втрати при передачі кожного символу a_i визначає приватна умовна ентропія джерела $H(B/a_i)$:

$$H(B/a_i) = -\sum_{j=1}^{3} p(b_j/a_i) \log p(b_j/a_i), (i = 1,2,3), \text{ біт/символ},$$

$H(B/a_1) = -(0{,}98 \log 0{,}98 + 0{,}01 \log 0{,}01 + 0{,}01 \log 0{,}01) =$
$= 0{,}0286 + 0{,}0664 + 0{,}0664 = 0{,}1614$, *біт/символ,*

$H(B/a_2) = -(0{,}10 \log 0{,}10 + 0{,}75 \log 0{,}75 + 0{,}15 \log 0{,}15) =$
$= 0{,}3322 + 0{,}3113 + 0{,}4105 = 1{,}0540$, *біт/символ,*

$H(B/a_3) = -(0{,}20 \log 0{,}20 + 0{,}30 \log 0{,}30 + 0{,}50 \log 0{,}50) =$
$= 0{,}4644 + 0{,}5211 + 0{,}5000 = 1{,}4855$, *біт/символ*.

5. Середні втрати інформації при передачі одного символу визначає загальна умовна ентропія джерела $H(B/A)$:

$$H(B/A) = -\sum_i \sum_j p(a_i)\, p(b_j/a_i) \log p(b_j/a_i) =$$
$$= -[0{,}7(0{,}98 \log 0{,}98 + 0{,}01 \log 0{,}01 + 0{,}01 \log 0{,}01) +$$
$$+ 0{,}2(0{,}10 \log 0{,}10 + 0{,}75 \log 0{,}75 + 0{,}15 \log 0{,}15) +$$
$$+ 0{,}1(0{,}20 \log 0{,}20 + 0{,}30 \log 0{,}30 + 0{,}50 \log 0{,}50)] =$$
$$= 0{,}465 \quad \text{біт / символ}.$$

Загальні втрати інформації в каналі зв'язку при передачі повідомлення з 400 символів ΔI

$$\Delta I = k\, H(B/A) = 400 \times 0{,}465 = 186 \text{ біт},$$

де k - кількість символів у переданому повідомлені.

6.Безумовні імовірності появи сигналів на вході приймача $p(b_j)$ визначаються за формулою:

$$p(b_j) = \sum_i p(a_i)\, p(b_j/a_i), (j = 1,2,3),$$

$$p(b_1) = \sum_i p(a_i)\, p(b_1/a_i) = 0{,}7 \cdot 0{,}98 + 0{,}2 \cdot 0{,}10 + 0{,}1 \cdot 0{,}20 = 0{,}726,$$
$$p(b_2) = \sum_i p(a_i)\, p(b_2/a_i) = 0{,}7 \cdot 0{,}01 + 0{,}2 \cdot 0{,}75 + 0{,}1 \cdot 0{,}30 = 0{,}187,$$
$$p(b_3) = \sum_i p(a_i)\, p(b_3/a_i) = 0{,}7 \cdot 0{,}01 + 0{,}2 \cdot 0{,}15 + 0{,}1 \cdot 0{,}50 = 0{,}087.$$

Перевіримо, чи складають імовірності $p(b_j)$ повну групу, тобто $\sum_j p(b_j) = 1$

$$\sum_j p(b_j) = 0{,}726 + 0{,}187 + 0{,}087 = 1.$$

7. Середня кількість інформації, прийнята приймачем на один символ, визначається ентропією приймача $H(B)$

$$H(B) = -\sum_j p(b_j) \log\, p(b_j) =$$

$$= -(0{,}726 \log 0{,}726 + 0{,}187 \log 0{,}187 + 0{,}087 \log 0{,}087) = 1{,}095 \text{ біт/символ}.$$

8. Максимальна ентропія приймача, $H_{max}(B)$

$$H_{max}(B) = \log N = \log 4 = 2 \text{ біт/символ.}$$

9. Середня кількість отриманої приймачем інформації, отримана приймачем на один символ з урахуванням втрат інформації ураженої завадами, $I(A, B)$

$$I(A, B) = H(B) - H(B / A) = 1{,}095 - 0{,}465 = 0{,}63 \text{ біт/символ}.$$

10. Швидкість модуляції дискретного джерела повідомлень, n

$$\text{n} = \frac{1}{\tau} = \frac{1}{0{,}0002} = 5000, \text{ біт.}$$

Примітка: Якщо тривалість передачі сигналів різна ($\tau_1 \neq \tau_2 \neq \tau_3$), то розраховують середню тривалість передачі $\tau_{ср}$

$$\tau = \tau_{ср} = \sum_{ш=1}^{3} p(a_i)\tau_i \text{ , сек.}$$

11. Продуктивність дискретного джерела повідомлень, $H'(A)$

$$H'(A) = \frac{H(a)}{\tau} = \frac{1{,}1568}{0{,}0002} = 5784 \text{ бод.}$$

12. Швидкість передачі інформації, R

$$R = \frac{H(A) - H(A/B)}{\tau} \text{ або } R = \frac{H(B) - H(B/A)}{\tau}$$

у нашому випадку швидкість дорівнює

$$R=\frac{H(B)-H(B/A)}{\tau}=\frac{1{,}0950-0{,}4650}{0{,}0002}=3150\ бод.$$

13. Пропускна здатність (ємкість) C дискретного каналу зв'язку визначається максимальною швидкістю передачі $C=max\ R$

$$C=\frac{H_{max}(A)-H(A/B)}{\tau}\ \text{або}\ C=\frac{H_{max}(B)-H(B/A)}{\tau}$$

у нашому випадку

$$C=\frac{H_{max}(B)-H(B/A)}{\tau}=\frac{2-0{,}4650}{0{,}0002}=7675\ бод.$$

14. Коефіцієнт ефективності дискретного каналу зв'язку, $K_э$

$$K_э=\frac{R}{C}=\frac{3150}{7675}=0{,}41.$$

15. Критична швидкість передачі $R_{кр}$

$$R_{кр}=\frac{C}{H(A)}=\frac{7675}{1{,}1568}=6635\ бод.$$

Отже виконуються теореми Шеннона про швидкість передачі ($R>R_{кр}$, $3150>6635$ *бод*), та про кодування ($H'(A)<C$, $5784<7675$, *бод*).

Резюме. Наданий дискретний канал має високі інформаційні характеристики, а виконання теорем Шеннона свідчить про його надійність, та ефективність.

Задача вирішена.

У випадку опису перешкод каналу зв'язку канальною матрицею об'єднання виду $p(a_i/b_j)$, можливостей для обчислення інформаційних характеристик ще більше. У задачі послідовно обчислюємо:

1. Безумовні імовірності джерела $p(a_i)$

$$p(a_i)=\sum_j p(a_i,b_j)\quad (i=1,2,\ldots,m)$$

і перевіряємо, що імовірності складають повну групу, тобто сума $p(a_i)$ дорівнює одиниці.

2. Безумовну ентропію джерела $H(A)$

$$H(A) = -\sum_i \sum_j p(a_i, b_j) \log \sum_j p(a_i, b_j) = -\sum_i p(a_i) \log\, p(a_i)\ \textit{біт/символ.}$$

3. Безумовні імовірності приймача $p(b_j)$

$$p(b_j) = \sum_i p(a_i, b_j) \quad (i = 1, 2, \ldots, m)$$

і перевіряємо, що імовірності складають повну групу, тобто сума $p(b_i)$ дорівнює одиниці.

4. Безумовну ентропію приймача $H(B)$

$$H(B) = \sum_i \sum_j p(a_i, b_j) \log \sum_i p(a_i, b_j) = -\sum_j p(b_j) \log\, p(b_j)\text{, } \textit{біт/симв.}$$

5. Умовні імовірності джерела $p(b_j / a_i)$ або умовні імовірності приймача $p(a_i / b_j)$, та будуємо відповідні канальні матриці джерела, або приймача

$$p(b_j / a_i) = \frac{p(a_i, b_j)}{\sum_j p(a_i, b_j)} = \frac{p(a_i, b_j)}{p(a_i)} \quad \begin{pmatrix} i = 1,2,\ldots,m \\ j = 1,2,\ldots,m \end{pmatrix}$$

або

$$p(a_i / b_j) = \frac{p(a_i, b_j)}{\sum_i p(a_i, b_j)} = \frac{p(a_i, b_j)}{p(b_j)} \quad \begin{pmatrix} i = 1,2,\ldots,m \\ j = 1,2,\ldots,m \end{pmatrix}.$$

6. Інформаційні втрати при передачі кожного символу

$$H(B / a_i) = -\sum_j \mathrm{p(b_j/a_i) \log p(b_j/a_i)},\ (\mathrm{i = 1,2,3 \ldots m})\text{, } \textit{біт/символ.}$$

7. Середні втрати інформації при передачі одного сигналу, що визначає загальна умовна ентропія джерела $H(B / A)$

$$H(B / A) = -\sum_i \sum_j p(a_i)\, p(b_j / a_i) \log\, p(b_j / a_i)\ \textit{біт/символ}$$

або загальна умовна ентропія приймача повідомлень $H(A / B)$

$$H(A / B) = -\sum_i \sum_j p(b_j)\, p(a_i / b_j) \log\, p(b_j / a_i)\ \textit{біт/символ.}$$

8. Загальні втрати інформації в каналі зв'язку при передачі k символів повідомлення

$$\Delta I = kH(B / A),\ \textit{біт.}$$

9. Середня кількість інформації, отримана приймачем на один символ з

урахуванням перешкод каналу зв'язку, $I(A,B)$:

$$I(A,B) = H(B) - H(B/A), \textit{ біт/символ}$$

або

$$I(A,B) = H(A) - H(A/B), \textit{ біт/символ.}$$

10. Швидкість модуляції дискретного джерела повідомлень, n

$$\text{n} = \frac{1}{\tau}, \textit{ бод.}$$

Примітка. Якщо тривалість передачі сигналів різна ($\tau_1 \neq \tau_2 \neq \tau_3$), то розраховують середню тривалість передачі $\tau_{ср}$

$$\tau = \tau_{ср} = \sum_{ш=1}^{3} p(a_i)\tau_i, \textit{ сек.}$$

11. Продуктивність дискретного джерела повідомлень, *H'(A)*

$$H'(A) = \frac{H(a)}{\tau} \textit{ бод.}$$

12. Швидкість передачі інформації, *R*

$$R = \frac{H(A) - H(A/B)}{\tau} \quad \text{або} \quad R = \frac{H(B) - H(B/A)}{\tau} \textit{ бод.}$$

13. Пропускна здатність *C* дискретного каналу зв'язку визначається максимальною швидкістю передачі *C=max R*

$$\text{C} = \frac{H_{max}(A) - H(A/B)}{\tau} \quad \text{або} \quad \text{C} = \frac{H_{max}(B) - H(B/A)}{\tau} \textit{ бод.}$$

14. Коефіцієнт ефективності дискретного каналу зв'язку, $K_э$

$$K_э = \frac{R}{C}.$$

15. Критична швидкість передачі $\text{R}_{кр}$

$$\text{R}_{кр} = \frac{C}{H(A)} \textit{ бод.}$$

Резюме. Дати оцінку інформаційних характеристик дискретного каналу,

виконання теорем Шеннона про швидкість та кодування. Дати оцінку надійності та ефективності каналу.

3.2. Оптимальне кодування

Основною характеристикою дискретного каналу зв'язку є швидкість передачі даних. При надмірності переданого повідомлення швидкість передачі зменшується. Для виключення надмірності повідомлення використовують математичні, та програмні засоби компресії даних без втрат змісту інформації, в тому числі оптимальне кодування.

Оптимальне кодування застосовується для стиснення (компресії даних), що дозволяє ефективно використовувати пам'ять ЕОМ, виконувати архівацію даних, зменшити тривалість, та збільшити швидкість передачі повідомлень, зменшити дію завад на інформацію.

3.2.1. Оптимальний нерівномірний код Шеннона-Фано

Основний ідея оптимального кодування полягає в тому, що символам повідомлення, які мають велику імовірність, привласнюються короткі бінарні коди, тобто утворюються бінарні кодові слова різної довжини - нерівномірні коди. Оптимальним нерівномірним кодом (ОНК) називається такий код, для якого середня довжина коду є мінімальною.

Для однозначності кодування і декодування оптимальних нерівномірних кодів необхідно, щоб вони були префіксними, тобто для них повинен виконуватися критерій Фано: ні яке кодове слово ОНК не є початком іншого кодового слова ОНК.

Побудова ОНК Шеннона-Фано. Бінарний оптимальний нерівномірний код (ОНК) Шеннона-Фано будується ітераційним методом бісекції (дихотомії) в кілька кроків:

Попередній крок. Символи повідомлення x_i ранжируються в порядку убування їхніх ймовірностей (або їх збільшення) p (x_i);

Крок 1. Символи x_i розбиваються на дві секції, із приблизно рівними сумарними ймовірностями;

Крок 2. Символам 1-ої секції привласнюється перший біт ОНК якій, дорівнює нулеві, а 2-й секції – біт ОНК, який дорівнює одиниці;

Крок 3. Кожну секцію знову поділяємо на дві рівноімовірні підсекції. Символам перших підсекцій привласнюється другий біт ОНК, який дорівнює нулеві, а другим підсекціям – біт ОНК, який дорівнює одиниці.

Таке ділення на усе більш дрібні секції проводиться доти, поки у кожній із секцій лишиться по одному символу, тобто бінарні кодові слова будуть побудовані.

Для оцінки ефективності побудованого ОНК необхідно обчислити наступні показники:

1. ***Середня довжина ОНК,*** $l_{ср}$

$$l_{ср} = \sum_{i=1}^{n} l_i \, p(x_i), \; біт,$$

де l_i – довжина ОНК символу x_i;

$p(x_i)$- імовірність символу x_i

2. ***Ентропія повідомлення***, *H(X)*

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log\, p(x_i)\,, \text{ біт/символ.}$$

3. ***Відносна ентропія*** ОНК, μ

$$\mu = \frac{H}{H_{\max}} = \frac{-\sum_{i=1}^{n} p(x_i) \log\, p(x_i)}{\log N},$$

де H - ентропія ОНК;

$H_{\max}$ = максимальна ентропія, $H_{\max} = \log N$;

N - загальна кількість переданих символів повідомлення.

4. ***Інформаційна надмірність*** *D*, що показує відносне недовантаження на символ коду

$$D = 1 - \frac{H}{H_{\max}} = 1 - \mu\,.$$

5. ***Абсолютне недовантаження*** на символ повідомлень, ΔD

$$\Delta D = (H_{\max} - H), \textit{ біт/символ.}$$

6. ***Коефіцієнт статистичного стиску*** *Кс.*, що характеризує зменшення кількості бінарних знаків на символ повідомлення при застосуванні ОНК

$$K_{c.} = 1 - \frac{l_{ср}}{l_{рбк}},$$

де $l_{рбк}$ – довжина рівномірного коду.

7. ***Коефіцієнт відносної ефективності ОНК.*** $K_э$, що показує ступінь використання статистичної надмірності переданого повідомлення

$$K_э = \frac{H}{l_{ср}}.$$

Шеннон показав, що повідомлення може бути закодоване так, що середня довжина нерівномірного коду $l_{ср}$ наближається до ентропії Н ($l_{ср} \geq$Н). Таким чином, ентропія дозволяє оцінити ступень наближення нерівномірного коду до оптимального.

Задача. Побудувати рівномірний бінарний код і ОНК методом Шеннона-Фано для символів повідомлення a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, імовірності появи яких складають повну групу:

$p(a_1) = p(a_2) = 0{,}25$; $p(a_3) = p(a_4) = 0{,}125$; $p(a_5) = p(a_6) = p(a_7) = p(a_8) = 0{,}0625$.

Побудувати кореневі бінарні дерева РБК, та ОНК. Обчислити інформаційні характеристики ОНК, оцінити його ефективність та

оптимальність.

Рішення

Перевіряємо імовірності $p(a_i)$ на повноту групи, тобто $\sum_{i=1}^{8} p(a_i) = 1$

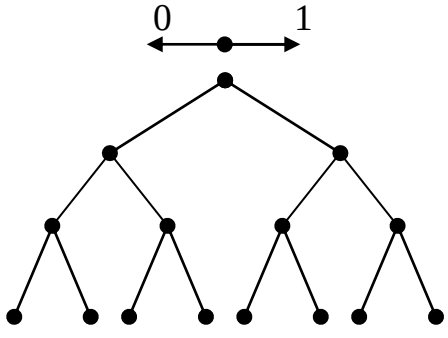
$$\sum_{i=1}^{8} p(a_i) = 2 \cdot 0{,}25 + 2 \cdot 0{,}125 + 4 \cdot 0{,}0625 = 1.$$

Ранжируємо імовірності в порядку їхнього убування. Застосовуючи послідовно метод бісекції, будуємо кроки розподілу, поки в кожній секції залишиться по одному символу. Складаємо варіанти бінарних кодів: рівномірний, ОНК і інверсний ОНК. Результати обчислень зводимо в табл. 3.1.

Таблиця 3.1

a_i	p_i	рівномірний код	1-й крок 1-й біт	2-й крок 2-й біт	3-й крок 3-й біт	4-й крок 4-й біт	ОНК	l_i *біт*	$l_i p_i$	H	інверсний ОНК
a_1	0,25	000	$I \Rightarrow 0$	$I \Rightarrow 0$			00	2	0,5	0,5	11
a_2	0,25	001		$I \Rightarrow 1$			01	2	0,5	0,5	10
a_3	0,125	010	$I \Rightarrow 1$	$I \Rightarrow 0$	$I \Rightarrow 0$		100	3	0,375	0,375	011
a_4	0,125	011			$I \Rightarrow 1$		101	3	0,375	0,375	010
a_5	0,0625	100		$I \Rightarrow 1$	$I \Rightarrow 0$	$I \Rightarrow 0$	1100	4	0,25	0,25	0011
a_6	0,0625	101				$I \Rightarrow 1$	1101	4	0,25	0,25	0010
a_7	0,0625	110			$I \Rightarrow 1$	$I \Rightarrow 0$	1110	4	0,25	0,25	0001
a_8	0,0625	111				$I \Rightarrow 1$	1111	4	0,25	0,25	0000
	$\sum_i p_i = 1$	—					—	—	$l_{ср}$ = = 2,75	H = = 2,75	—

Будуємо кореневі бінарні дерева рівномірного коду і ОНК Шеннона-Фано, Рис. 3.1 і Рис.3.2 і задаємо напрям визначення бітів РБК та ОНК



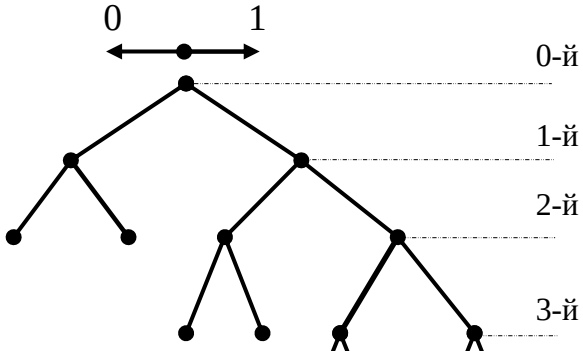


Рис. 3.2. *Кореневе дерево IV порядку ОНК Шеннона-Фано*

Побудований ОНК Шеннона-Фано має властивість однозначного декодування, тому що для нього виконується критерій Фано і всі кодові слова є кінцевими вузлами кореневого дерева.

Обчислюємо показники ефективності ОНК.

1. Середня довжина ОНК $\sum_{i=1}^{8} l_i p(a_i) = 2{,}75$ *біт.*

2. Ентропія ОНК $H = -\sum_{i=1}^{8} p(a_i) \cdot \log p(a_i) = 2{,}75$ *біт/символ.*

Значення - $p(a_i)$ log $p(a_i)$ вибираємо з таблиці ентропії додатка 2, а значення $\log_2 8$ з додатка 1.

3. Максимальна ентропія

$$H_{\max} = \log N = \log_2 8 = 3 \text{ біт/символ.}$$

4 Відносна ентропія

$$\mu = \frac{H}{H_{\max}} = \frac{2{,}75}{3} = 0{,}92 .$$

5. Інформаційна надмірність

$$D = 1 - \frac{H}{H_{\max}} 1 - 0{,}92 = 0{,}08 .$$

6. Абсолютне недовантаження

$$\Delta D = H_{\max} - H = 3 - 2{,}75 = 0{,}25 \text{ біт/символ.}$$

7. Коефіцієнт стиснення інформації

$$K_c = 1 - \frac{l_{ср}}{l_{рбк}} = 1 - \frac{2{,}75}{3} = 0{,}09 \Rightarrow 9\% .$$

8. Коефіцієнт відносної ефективності

$$K_э = \frac{H}{l_{ср}} = \frac{2{,}75}{2{,}75} = 1 .$$

Побудований ОНК Шеннона-Фано має високі інформаційні характеристики, а $К_э = 1$, отже, цей код є ефективним та оптимальним.

Задача вирішена.

3.2.2. Побудова оптимального нерівномірного коду Хаффмена

Кодування по методу Хаффмена здійснюється у кілька кроків:

Попередній крок. Повідомлення - x_i розташовуємо в порядку убування їхніх ймовірностей $p(x_i)$.

*Крок 1.*Робимо перший стиск (“склеювання”) двох символів, тобто групуємо разом два символи, що мають найменшу імовірність й обчислюємо їхню загальну імовірність. Отримуємо новий об’єднаний символ.

Крок 2. Робимо другий стиск. Знову групуємо разом два символи, що мають найменші імовірності й обчислюємо їхню загальну імовірність, проводимо єднаючи лінії.

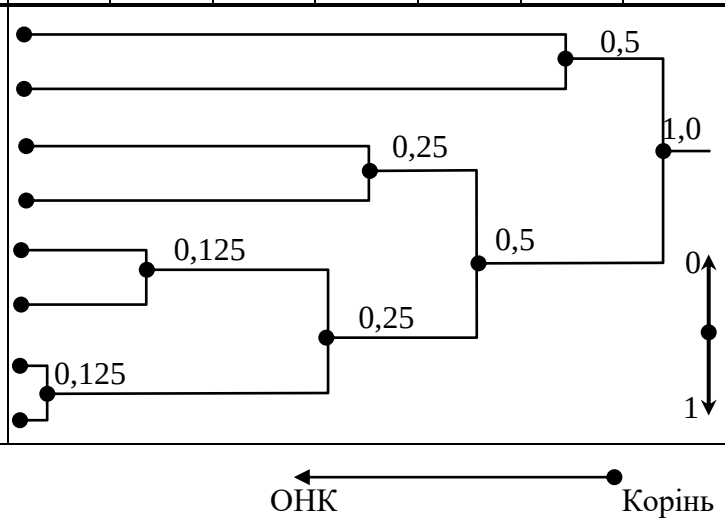
І так далі, процес покрокового стиску символів здійснюється доти поки в ансамблі повідомлення лишається один об’єднаний символ з імовірністю $p=1$ (кореневий вузол). При цьому утворюється кореневе бінарне дерево ОНК Хаффмана, гілки якого з’єднують кореневий вузол з кінцевими вузлами (початковими символами повідомлення).

Крок завершальний. Кодові слова ОНК одержуємо пересуваючись по гілкам кореневого дерева від кореня до кінцевих вузлів. При цьому кожне ребро дерева визначає біт ОНК (0 або 1) відповідно до напряму значень бітів кореневого дерева.

Усі побудови ОНК Хаффмена і розрахунок його інформаційних характеристик зручно оформити у виді табл.3.2 Для заданого варіанта повідомлень (дивись попередню задачу) необхідно побудувати рівномірний код і кілька варіантів ОНК Хаффмена, побудувати кореневі дерева РБК та ОНК, обчислити інформаційні характеристики і показники ефективності ОНК Хаффмена.(див. приклад ОНК Шеннона-Фано).

Таблиця 3.2

a_i	p_i	рівномірний код	1-й крок	2-й крок	3-й крок	4-й крок	5-й крок	6-й крок	7-й крок	ОНК
a_1	0,25	000								00
a_2	0,25	001								01
a_3	0,125	010								100
a_4	0,125	011								101
a_5	0,0625	100								1100
a_6	0,0625	101								1101
a_7	0,0625	110								1110
a_8	0,0625	111								1111



Задача вирішена.

3.3. Завадостійке кодування

Наявність шумів у реальних каналах зв'язку зменшує надійність інформації за рахунок перекручування і втрат при передачі даних. Надійність інформації це імовірність правильного прийому повідомлень з урахуванням впливу перешкод. Надійність зв'язана з завадостійкістю й ефективністю, побудовою що виявляють і коректують коди.

Бінарний код стає завадостійким завдяки введенню додаткової надмірності (контрольних біт). Завадостійкі коди поділяються на два класи: коди, що виявляють помилки, та коригуючи коди.

Коди, що виявляють помилки дозволяють тільки встановити наявність одної або кількох помилок, але розрахувати адрес помилки вони не можуть. До цих кодів відносяться: коди парності, коди інверсії, коди подвоєння, СТК№3 та інші.

3.3.1. Коригуючий систематичний код Хеммінга

Найбільший інтерес представляють коригувальні коди, які дозволяють не тільки знайти, але і виправити помилку.

Коригуючий систематичний код Хеммінга (КСКХ) дозволяє визначити та коригувати одну помилку. КСКХ є щільноупакованим кодом, тому що має мінімальну надмірність, контрольні біти включаються у середину інформаційної часті бінарного слова. КСКХ генеруються за допомогою або правил парності, або твірної матриці.

Розглянемо приклад побудови щільноупакованого КСКХ за правилами

парності.

Задача. Побудувати коригуючий систематичний код Хемминга для виявлення і виправлення помилки для інформаційної комбінації 0101.

Рішення. Виконаємо генерацію, діагностику, коригування і декоригування.

1. Генерація КСКХ.

Кількість інформаційних біт $n_i = 4$. Кількість контрольних бітів n_k визначається за таблицею №1 додатку №3: $n_к = 3$. Загальна довжина коригуючого коду n дорівнює

$$n = n_i + n_к = 4 + 3 = 7 \text{ біт.}$$

Номера j позицій $П_j$ для контрольних біт K_i обчислюється як $j=2^{i-1}$:

для K_1, $i=1$, тоді $j=2^{1-1}=2^0=1$, тобто K_1 знаходиться у позиції $П_1$;
для K_2, $i=2$, тоді $j=2^{2-1}=2^1=2$, тобто K_2 знаходиться у позиції $П_2$;
для K_3, $i=3$, тоді $j=2^{3-1}=2^2=4$, тобто K_3 знаходиться у позиції $П_4$;
для K_4, $i=4$, тоді $j=2^{4-1}=2^3=8$, тобто K_4 знаходиться у позиції $П_8$;
для K_5, $i=5$, тоді $j=2^{5-1}=2^4=16$, тобто K_5 знаходиться у позиції $П_{16}$.

Складемо макет коду КСКХ і запишемо його в таблицю 3.3.

Таблиця 3.3

Позиції $П_j$	$П_1$	$П_2$	$П_3$	$П_4$	$П_5$	$П_6$	$П_7$
Макет КСКХ	$К_1$	$К_2$	0	$К_3$	1	0	1
Код КСКХ	0	1	0	0	1	0	1

Обчислимо значення контрольних біт $К_1$, $К_2$, $К_3$ за правилами перевірки на парність (табл. №3, додаток 3). Для цього макет КСКХ обробляється правилами парності додаючи по модулю два:

Правіло 1: $П_1 \oplus П_3 \oplus П_5 \oplus П_7 = К_1 \oplus 0 \oplus 1 \oplus 1 = 0$, сума парна при $К_1 = 0$;
Правіло 2: $П_2 \oplus П_3 \oplus П_6 \oplus П_7 = К_2 \oplus 0 \oplus 0 \oplus 1 = 0$, сума парна при $К_2 = 1$;
Правіло 3: $П_4 \oplus П_5 \oplus П_6 \oplus П_7 = К_3 \oplus 1 \oplus 0 \oplus 1 = 0$, сума парна при $К_3 = 0$.

Побудований коригувальний код запишемо в таблицю 3.3.

2. Діагностика. Нехай, у каналі зв'язку під дією перешкод замість 0100101 було прийнято 0100111. Прийнятий коригуючий код КСКХ обробляється правилами парності і визначається адрес помилки:

Правіло 1: $П_1 \oplus П_3 \oplus П_5 \oplus П_7 = 0 \oplus 0 \oplus 1 \oplus 1 = 0$, молодшій розряд адреси

помилки (АП), дорівнює 0;

Правіло 2: $П_2 \oplus П3 \oplus П6 \oplus П_7 = 1 \oplus 0 \oplus 1 \oplus 1 = 1, \Rightarrow$ АП = 1;

Правіло 3: $П_4 \oplus П_5 \oplus П_6 \oplus П_7 = 0 \oplus 1 \oplus 1 \oplus 1 = 1 \Rightarrow$ АП = 1.

Бінарний адрес помилкової позиції читається знизу уверх і дорівнює 110, що відповідає позиції $П_6$ у десятинній системі. Отже, помилка в символі 6-й позиції.

3. Коригування. Помилковий розряд треба змінити на інверсний та одержимо правильну кодову комбінацію КСКХ.

4. Декодування. Із коригуючого коду видаляються контрольні біти.

Задача вирішена.

Код Хемминга може бути використаний для побудови коду з виправленням одиночної помилки і виявленням подвійної. Для цього, крім зазначених вище перевірок за контрольним позиціям, проводять ще одну перевірку на парність для всього рядка в цілому. Щоб здійснити таку перевірку, треба до кожного рядка коду додати контрольні символи, записані в додаткової 8-й позиції. Тоді у випадку однієї помилки перевірки за позиціям вкажуть помилкової позиції, а перевірка на парність - на наявність другої помилки. Якщо перевірки позиції вкажуть на наявність помилки, а перевірка на парність її не фіксує, значить у кодовій комбінації дві помилки.

3.3.2. Коригуючий циклічний код

Задача. Для бінарного слова 1001100 побудувати коригуючий циклічний код (КЦК).

Генерація КЦК за допомогою твірного поліному $g(x)= x^9+x^8+x^1+1$.

Надано бінарне слово, можна представити, як поліном Q(x)

$$К - 1001100 \Rightarrow x^6 + x^3 + x^2 = Q(x).$$

Макет КЦК будується шляхом зсуву ісходника Q(x) на 9 біт вліво, тим самим резервуємо позиції для контрольних біт $k_1,k_2,\ldots,k_9$

$$Q(x) \cdot x^9 = (x^6 + x^3 + x^2) \cdot x^9 = x^{15} + x^{12} + x^{11}.$$

Макет КЦК у бінарній формі має вигляд $\overbrace{1001100}^{Nu=7бит}\underbrace{000000000}_{k_1k_2k_3k_4k_5k_6k_7k_8k_9}^{Nк=9бит}$.

Твірний поліном g(x) у бінарній формі має вигляд

$$g(x) = x^9 + x^8 + x + 1 \Rightarrow \overbrace{1100000011}^{g(x)=10бит}.$$

Макет КЦК ділимо по модулю два на твірний поліном і залишок m(x) визначає значення контрольних біт

$$
\begin{array}{l}
1001100000000000/1100000011 \\
\oplus\underline{1100000011} \\
\quad 1011000110 \\
\oplus\underline{1100000011} \\
\quad 1110001010 \\
\oplus\underline{1100000011} \\
\quad 1000100100 \\
\oplus\underline{1100000011} \\
\quad 1001001110 \\
\oplus\underline{1100000011} \\
\quad 1010011010 \\
\oplus\underline{1100000011} \\
\quad 110011001 = \mathrm{m(x)} \ \text{залишок.}
\end{array}
\qquad
\begin{array}{l}
K_1 = 1 \\
K_2 = 1 \\
K_3 = 0 \\
K_4 = 0 \\
K_5 = 1 \\
K_6 = 1 \\
K_7 = 0 \\
K_8 = 0 \\
K_9 = 1
\end{array}
$$

Отже коригуючий циклічний код має вигляд $\overbrace{1001100}^{Nu=7бит}\overbrace{110011001}^{Nк=9бит}$.

Діагностика. КЦК визначає і коригує одиничну помилку.

Прийнятий КЦК ділимо по модулю два на твірний поліном g(x) і помилка визначається по залишку m(x):

а) m(x) = 0 $\Rightarrow$ помилки не має;

б) m(x) має одну одиницю $\Rightarrow$ одиниця визначає адресу помилкового контрольного біта k_j;

в) m(x) має обрамлення, в середині якого є одна одиниця $\Rightarrow$ одиниця визначає адресу помилки інформаційного біта, позицію $П_i$

г) всі інші форми залишку m(x) $\Rightarrow$ кратна помилка адреса якої не визначається.

Припустимо, що під час прийому коригуючого коду з’явилась помилка в інформаційній частині КЦК $\overbrace{100111}^{Nu=7бит}\overbrace{0110011001}^{Nк=9бит}$. Визначимо адресу цієї помилки. Прийнятий КЦК ділимо по модулю два на твірний поліном g(x)

$$
\begin{array}{l}
1001110110011001/1100000011 \\
\oplus\underline{1100000011} \\
\quad 1011101010 \\
\oplus\underline{1100000011} \\
\quad 1111010011 \\
\oplus\underline{1100000011} \\
\quad 1101000010 \\
\oplus\underline{1100000011} \\
\quad 10000010\,|\,1 = m(x).
\end{array}
$$

Залишок m(x) має обрамлення, всередині якого є одна одиниця, яка визначає адрес помилки в інформаційній частині, АП=$П_6$.

Припустимо, що під час прийому коригуючого коду з’явилася помилка в

контрольній частині $\overbrace{1001100}^{Nu=7бит}\overbrace{110010001}^{Nк=9бит}$. Визначимо адресу цієї помилки. Для цього ділимо прийнятий КЦК на твірний поліном g(x)

$$
\begin{array}{l}
1001100110010001/1100000011 \\
\oplus\ \underline{1100000011} \\
\quad 1011001010 \\
\oplus\ \underline{1100000011} \\
\quad 1110010011 \\
\oplus\ \underline{1100000011} \\
\quad 1001000000 \\
\oplus\ \underline{1100000011} \\
\quad 1010000110 \\
\oplus\ \underline{1100000011} \\
\quad 1100001011 \\
\oplus\ \underline{1100000011} \\
\quad 000001000 = m(x).
\end{array}
$$

Залишок m(x) має одну одиницю тобто помилка в контрольній частині коду, k_6, що відповідає адресу помилки $П_{13}$.

5.3.3. Генерація коригуючого циклічного коду за допомогою твірної матриці

Генеруємо коригуючий циклічний код для ісходника К – 1001100.

Будуємо одиничну матрицю Е

$$
E(n_u \times n_u); E = \begin{Vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{Vmatrix}.
$$

Будуємо перевірочну матрицю R

$$
R(n_u \times n_n) \Rightarrow (7 \times 9),
$$

де кількість контрольних біт n_k дорівнює $n_к = n_u + 2 = 7 + 2 = 9$ *біт.*

Перевірочна матриця містить всі синдроми помилок КЦК, що можливі в інформаційній частині коду.

$$R = \begin{Vmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{Vmatrix}.$$

Твірна матриця будується з'єднанням одиничної матриці E і перевірочної матриці – R

$$G = E \mid R = \begin{Vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{Vmatrix}.$$

Генеруємо коригуючий циклічний код для ісходника. Для цього ісходник помножимо по модулю два на твірну матрицю **G**

$$1001100 \cdot \begin{Vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{Vmatrix} = 1001100010011000.$$

Отже коригуючий циклічний код для наданого ісходника має вигляд 1001100010011000.

3.4. Криптографічне кодування

Інформація стала економічною категорією, самим дорогим товаром. Тому інформація потребує захисту від несанкціонованого доступу. Методи захисту інформації вивчає наука криптологія, яка складається з двох частин:

- *криптографія* – створення методів захисту інформації від несанкціонованого доступу;
- *кріптоаналіз* – створення методів "злому" систем захисту інформації.

Криптографія по захисту інформації від несанкціонованого доступу вирішує слідуючи задачі:

1. Конфіденційність;
2. Оперативність доступу для санкціонованого користувача;
3. Автентичність;
4. Цілісність;
5. Юридична значимість;
6. Невідслідкованість;
7. Криптостійкість шифру.

Криптографічні методи розподіляються на класи:

1. Поточні;
2. Блочні;
3. Багатоалфавітні;
4. Симетричні криптосистеми;
5. Відкриті криптосистеми;
6. Електронний цифровий підпис.

Криптографічні методи вивчаються у окремій дисципліні та не входять до складу даних методичних вказівок.

4. КОНТРОЛЬНІ ПИТАННЯ ДЛЯ САМОПІДГОТОВКИ

Питання складені відповідно до робочої програми і можуть бути використані для самостійної підготовки студентів.

Теорія інформації

1. Основні класи задач теорії інформації, їхня актуальність, фактори ефективності використання комп'ютерних мереж. Кількісна оцінка інформації.
2. Передача інформації по каналу зв'язку, структура джерела, лінії зв'язку, приймача, дискретні і безперервні канали зв'язку.
3. Дискретні і безперервні канали зв'язку, апроксимація безперервних повідомлень дискретними сигналами, квантування, крок квантування, теорема Котельникова про квантування.
4. Дискретизація безперервних повідомлень, розгорнення і квантування цифрової, текстової, аудіо і відео інформації.
5. Міра кількості інформації, її властивості.
6. Безумовна ентропія джерела інформації, діапазон зміни ентропії, максимальна ентропія її властивості.
7. Приватна умовна ентропія каналу, обчислення інформаційних втрат при передачі по реальному каналі зв'язку.

8. Загальна умовна ентропія каналу, обчислення інформаційних втрат при передачі по реальному каналі зв'язку.
9. Канальна матриця джерела, її структура і властивості, приватна і загальна умовна ентропія джерела.
10. Канальна матриця приймача, її структура і властивості, приватна і загальна умовна ентропія приймача.
11. Канальна матриця об'єднання, її структура і властивості, обчислення інформаційних характеристик.
12. Взаємозв'язок канальних матриць джерела і приймача, обчислення інформаційних характеристик каналу зв'язку.
13. Три способи опису каналу зв'язку канальними матрицями.
14. Взаємозв'язок канальної матриці приймача і канальної матриці об'єднання, обчислення інформаційних характеристик.
15. Взаємозв'язок канальної матриці джерела і канальної матриці об'єднання, обчислення інформаційних характеристик.
16. Обчислення інформаційних характеристик реальних каналів зв'язку, безумовні ентропії джерела і приймача, приватні і загальні умовні ентропії.
17. Швидкість передачі інформації по ідеальному та реальному каналам зв'язку, одиниці виміру швидкості.
18. Швидкість модуляції та пропускна здатність дискретного джерела повідомлень.
19. Пропускна здатність (ємність) ідеального і реального каналів зв'язку, одиниці виміру.
20. Симетричний бінарний канал зв'язку, його властивості, безумовна й умовна ентропія.
21. Взаємозв'язок канальних матриць умовних ймовірностей джерела і приймача, обчислення безумовних і умовних ймовірностей, безумовних і умовних ентропій.
22. Теорема Шеннона про швидкість передачі повідомлень.
23. Теорема Шеннона про кодування повідомлень.

Теорія кодування

24. Оптимальне кодування, рівномірний і нерівномірний бінарні коди, оптимальні нерівномірні коди ОНК, інформаційні характеристики і фактори ефективності ОНК.
25. Алгоритм побудови ОНК Шеннона-Фано, кількість інформації, ентропія ансамблю, середня довжина бінарних слів ОНК, оцінка надмірності й ефективності ОНК.
26. Однозначність декодування ОНК, критерій Фано префіксності ОНК, кореневе бінарне дерево, інформаційні характеристики ОНК.
27. Алгоритм побудови ОНК Хаффмена, кількість інформації, ентропія ансамблю, середня довжина кодових слів, оцінка надмірності й ефективності ОНК.
28. Оптимальне кодування даних як засіб ефективного використання ЕОМ та

комп'ютерних мереж при передачі, обробці і збереженні даних; стиск даних, фактори ефективності компресії даних, архівація даних, інформаційні характеристики ОНК.

29. Завадостійке кодування, класифікація кодів, надмірність і щільність запакування кодів, використання їх у комп'ютерних мережах.
30. Коди, що виявляють помилки, алгоритми побудови кодів парності, інверсії, подвоєння, СТК №3.
31. Коригуючий комбінований інверсний код, алгоритм побудови, синдром помилки, обчислення адреси помилки, коректування помилки.
32. Генерація щільнозапакованого коригуючого систематичного коду Хеммінга (КСКХ) побудова макета коду, побудова правил парності обчислювання контрольних біт.
33. Коригуючий код КСКХ. Синдром помилки, обчислення адреси помилки, корегування помилки, декодування.
34. Генерація та діагностика коригуючого систематичного коду Хеммінга матрічним методом, розрахунок контрольних біт, та адреса помилки.
35. Коригуючи циклічні коди: генерація за допомогою твірного поліному, діагностика, корекція помилки, декодування, ефективність.
36. Генерація коригуючого циклічного коду за допомогою твірної матриці: діагностика, корекція помилки, декодування.
37. Коди, коригуючи кратні помилки: коди Боуза-Чоудхурі-Кохвінгема, твірні поліноми.
38. Генерація коригуючого мажоритарного коду КМК, діагностика, корекція помилок, декодування, та ефективність КМК.
39. Криптографічне кодування. Криптографія, та криптоаналіз, необхідність захисту інформації від несанкціонованого доступу.
40. Задачі криптографії, криптографічні принципи Шеннона, абсолютно стійкий ключ по Шеннону.
41. Поточні криптоалгорітми, їх класи, та особливості, прості, та складні заміни, криптостійкість, та ефективність.
42. Блочні криптоалгоритми, їх особливості, класифікація, види перестановок, та шифрів Кордана, криптостійкість, та ефективність.
43. Симетричні, багаторівневі криптосистеми ГОСТ, DES; криптостійкість, та ефективність, проблеми симетричних криптосистем.
44. Відкриті асиметричні криптосистеми, їх особливості, криптостійкість, та ефективність.
45. Електронний цифровий підпис, аутентичність електронних документів, та абонентів комп’ютерної мережі, електронні платіжні системи.

5. ВАРІАНТИ КОНТРОЛЬНИХ ЗАВДАНЬ

5.1. ВИБІР ВАРІАНТА КОНТРОЛЬНОГО ЗАВДАННЯ

Номер варіанта самостійної контрольної роботи визначається по ***сумі двох останніх цифр номеру залікової книжки студента, збільшеної на одиницю***. Наприклад, шифр студента 24859, сума двох останніх цифр 5 + 9 = 14, збільшивши її на одиницю, одержимо 14 + 1 = 15, отже, варіант роботи № 15.

У роботі студент виконує індивідуальні завдання №1, №2, №3. Виконуючи роботу, необхідно показати уміння правильно, коротко і чітко викладати навчальний матеріал. Робота повинна бути представлена на аркушах формату А4. На титульному листі вказується: найменування університету, факультету, кафедри, спеціальність, навчальна дисципліна, а також прізвище, ім'я і по батькові студента, його курс, група, та шифр варіанту роботи. Робота має бути виконана на персональному комп'ютері за допомогою офісного пакету програм (Microsoft Office та ін.).

Перед розв'язанням кожної задачі необхідно цілком навести її умови, зобразити малюнок, діаграму та дані відповідно до варіанта. Малюнки і діаграми повинні бути виконані акуратно з дотриманням вимог стандартів, у зручному для читання масштабі. Робота повинна бути підписана студентом з вказівкою дати виконання.

5.2. Завдання №1. Інформаційні характеристики дискретного каналу

Варіант 1. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(b_j / a_i) = \begin{Vmatrix} 0{,}90 & 0{,}10 & 0 & 0 \\ 0{,}05 & 0{,}94 & 0{,}01 & 0 \\ 0 & 0{,}01 & 0{,}98 & 0{,}01 \\ 0 & 0 & 0{,}10 & 0{,}90 \end{Vmatrix}.$$

Безумовні імовірності появи символів на виході джерела повідомлень дорівнює $p(a_1) = 0{,}6$; $p(a_2) = 0{,}2$; $p(a_3) = 0{,}1$; $p(a_4) = 0{,}1$. Тривалість передачі одного символу $\tau = 0{,}0002$ сек., передано повідомлення з 400 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 2. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(a_i / b_j) = \begin{Vmatrix} 0{,}90 & 0{,}10 & 0 & 0 \\ 0{,}05 & 0{,}84 & 0{,}01 & 0 \\ 0{,}03 & 0{,}06 & 0{,}98 & 0{,}10 \\ 0{,}02 & 0 & 0{,}01 & 0{,}90 \end{Vmatrix},$$

час передачі одного символу $\tau = 1$ м/сек., безумовні імовірності прийнятих повідомлень рівноімовірні. Передано повідомлення з 200 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 3. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(b_j / a_i) = \begin{Vmatrix} 0{,}97 & 0{,}03 & 0 & 0 \\ 0{,}01 & 0{,}98 & 0{,}01 & 0 \\ 0 & 0{,}02 & 0{,}96 & 0{,}02 \\ 0 & 0{,}02 & 0{,}03 & 0{,}95 \end{Vmatrix}.$$

Безумовні імовірності появи символів на виході джерела повідомлень дорівнює $p(a_1) = 0{,}4$; $p(a_2) = 0{,}4$; $p(a_3) = 0{,}1$; $p(a_4) = 0{,}1$. Тривалість передачі одного символу $\tau = 0{,}0002$ сек., передано повідомлення з 400 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 4. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(a_i / b_j) = \begin{Vmatrix} 0{,}99 & 0{,}02 & 0 & 0 \\ 0{,}01 & 0{,}98 & 0{,}01 & 0{,}01 \\ 0 & 0 & 0{,}98 & 0{,}02 \\ 0 & 0 & 0{,}01 & 0{,}97 \end{Vmatrix},$$

час передачі одного символу $\tau = 1$ м/сек., безумовні імовірності прийнятих повідомлень рівноімовірні. Передано повідомлення з 200 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 5. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(b_j / a_i) = \begin{Vmatrix} 0,98 & 0,01 & 0,01 & 0 \\ 0,15 & 0,75 & 0,10 & 0 \\ 0,25 & 0,20 & 0,50 & 0,05 \\ 0 & 0,02 & 0,03 & 0,95 \end{Vmatrix}.$$

Безумовні імовірності появи символів на виході джерела повідомлень дорівнює $p(a_1) = 0,4$; $p(a_2) = 0,2$; $p(a_3) = 0,1$; $p(a_4) = 0,3$. Тривалість передачі одного символу $\tau = 0,0002$ сек., передано повідомлення з 400 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 6. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(a_i / b_j) = \begin{Vmatrix} 0,90 & 0,05 & 0 & 0 \\ 0,10 & 0,94 & 0,01 & 0 \\ 0 & 0,01 & 0,98 & 0,10 \\ 0 & 0 & 0,01 & 0,90 \end{Vmatrix},$$

час передачі одного символу $\tau = 1$ м/сек., безумовні імовірності прийнятих повідомлень $p(b_1) = 0,15$; $p(b_2) = 0,25$; $p(b_3) = 0,28$; $p(b_4) = 0,32$. Передано повідомлення з 300 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 7. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(b_j / a_i) = \begin{Vmatrix} 0,98 & 0,02 & 0 & 0 \\ 0,01 & 0,97 & 0,01 & 0,01 \\ 0 & 0 & 0,98 & 0,02 \\ 0 & 0 & 0,01 & 0,99 \end{Vmatrix}.$$

Безумовні імовірності появи символів на виході джерела повідомлень дорівнює $p(a_1) = 0,4$; $p(a_2) = 0,3$; $p(a_3) = 0,2$; $p(a_4) = 0,1$. Тривалість передачі одного символу $\tau = 2$ м/сек., передано повідомлення з 250 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 8. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(a_i / b_j) = \begin{Vmatrix} 0,98 & 0,15 & 0,30 & 0 \\ 0,01 & 0,75 & 0,15 & 0,01 \\ 0,01 & 0,10 & 0,50 & 0,04 \\ 0 & 0 & 0,05 & 0,95 \end{Vmatrix},$$

час передачі одного символу $\tau = 1$ м/сек., безумовні імовірності прийнятих повідомлень $p(b_1) = 0,1$; $p(b_2) = 0,2$; $p(b_3) = 0,4$; $p(b_4) = 0,3$. Передано повідомлення з 150 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 9. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку.

$$p(b_j / a_i) = \begin{Vmatrix} 0,97 & 0,02 & 0,01 & 0 \\ 0 & 0,98 & 0,02 & 0 \\ 0,01 & 0,01 & 0,97 & 0,01 \\ 0 & 0 & 0,01 & 0,99 \end{Vmatrix}.$$

Безумовні імовірності появи символів на виході джерела повідомлень дорівнює $p(a_1) = 0,35$; $p(a_2) = 0,25$; $p(a_3) = 0,25$; $p(a_4) = 0,15$. Тривалість передачі одного символу $\tau = 2$ м/сек., передано повідомлення з 250 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 10. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(a_i / b_j) = \begin{Vmatrix} 0,98 & 0,01 & 0 & 0 \\ 0,02 & 0,97 & 0 & 0 \\ 0 & 0,01 & 0,98 & 0,01 \\ 0 & 0,01 & 0,02 & 0,99 \end{Vmatrix},$$

час передачі одного символу $\tau = 1$ м/сек., безумовні імовірності прийнятих повідомлень $p(b_1) = 0,3$; $p(b_2) = 0,1$; $p(b_3) = 0,4$; $p(b_4) = 0,2$. Передано повідомлення з 100 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 11. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(b_j / a_i) = \begin{Vmatrix} 0{,}90 & 0{,}05 & 0{,}03 & 0{,}02 \\ 0{,}10 & 0{,}84 & 0{,}06 & 0 \\ 0 & 0{,}01 & 0{,}98 & 0{,}01 \\ 0 & 0 & 0{,}10 & 0{,}90 \end{Vmatrix}.$$

Безумовні імовірності появи символів на виході джерела повідомлень дорівнює $p(a_1)$ = 0,25; $p(a_2)$ = 0,35; $p(a_3)$ = 0,15; $p(a_4)$ = 0,25. Тривалість передачі одного символу τ = 2,5 м/сек., передано повідомлення з 250 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 12. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(a_i / b_j) = \begin{Vmatrix} 0{,}97 & 0{,}01 & 0 & 0 \\ 0{,}03 & 0{,}98 & 0{,}04 & 0 \\ 0 & 0{,}01 & 0{,}95 & 0{,}01 \\ 0 & 0 & 0{,}01 & 0{,}99 \end{Vmatrix},$$

час передачі одного символу τ = 1,5 м/сек., безумовні імовірності прийнятих повідомлень $p(b_1)$ = 0,4; $p(b_2)$ = 0,3; $p(b_3)$ = 0,2; $p(b_4)$ = 0,1 . Передано повідомлення з 250 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 13. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(b_j / a_i) = \begin{Vmatrix} 0{,}75 & 0{,}01 & 0{,}20 & 0 \\ 0{,}10 & 0{,}98 & 0{,}28 & 0 \\ 0{,}15 & 0{,}01 & 0{,}50 & 0{,}03 \\ 0 & 0 & 0{,}02 & 0{,}97 \end{Vmatrix}.$$

Безумовні імовірності появи символів на виході джерела повідомлень дорівнює $p(a_1)$ = 0,25; $p(a_2)$ = 0,15; $p(a_3)$ = 0,35; $p(a_4)$ = 0,25. Тривалість передачі одного символу τ = 2 м4сек., передано повідомлення з 150 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 14. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(a_i / b_j) = \begin{Vmatrix} 0{,}97 & 0 & 0{,}01 & 0{,}01 \\ 0{,}02 & 0{,}98 & 0{,}01 & 0{,}03 \\ 0{,}01 & 0{,}02 & 0{,}96 & 0{,}02 \\ 0 & 0 & 0{,}02 & 0{,}94 \end{Vmatrix},$$

час передачі одного символу $\tau = 3$ м/сек., безумовні імовірності прийнятих повідомлень $p(b_1) = 0{,}2$; $p(b_2) = 0{,}3$; $p(b_3) = 0{,}4$; $p(b_4) = 0{,}1$. Передано повідомлення з 200 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 15. Надана: канальна матриця умовних ймовірностей, що віддзеркалюють дію завад дискретного каналу зв'язку

$$p(a_i / b_j) = \begin{Vmatrix} 0{,}98 & 0{,}02 & 0 & 0 \\ 0{,}02 & 0{,}97 & 0{,}01 & 0{,}02 \\ 0 & 0{,}01 & 0{,}96 & 0{,}03 \\ 0 & 0 & 0{,}03 & 0{,}95 \end{Vmatrix}.$$

Безумовні імовірності появи символів на виході джерела повідомлень дорівнює $p(a_1) = 0{,}33$; $p(a_2) = 0{,}27$; $p(a_3) = 0{,}14$; $p(a_4) = 0{,}26$. Тривалість передачі одного символу $\tau = 5$ м/сек., передано повідомлення з 100 символів.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$.

Варіант 16. Взаємозв'язок джерела з приймачем описано канальною матрицею спільних ймовірностей

$$p(A,B) = \begin{Vmatrix} 0{,}20 & 0 & 0 \\ 0{,}10 & 0{,}20 & 0 \\ 0 & 0{,}10 & 0{,}40 \end{Vmatrix},$$

час передачі одного символу $\tau = 0{,}0002$ сек.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$., якщо повідомлення складається з 300 символів.

Варіант 17. Взаємозв'язок джерела з приймачем описано канальною матрицею спільних ймовірностей

$$p(A,B) = \begin{Vmatrix} 0{,}25 & 0{,}10 & 0 \\ 0 & 0{,}20 & 0{,}10 \\ 0{,}15 & 0 & 0{,}20 \end{Vmatrix},$$

час передачі одного символу $\tau = 2$ м/сек.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$., якщо повідомлення складається з 250 символів.

Варіант 18. Взаємозв'язок джерела з приймачем описано канальною матрицею спільних ймовірностей

$$p(A,B) = \begin{Vmatrix} 0{,}10 & 0{,}10 & 0 \\ 0 & 0{,}20 & 0{,}10 \\ 0 & 0{,}20 & 0{,}30 \end{Vmatrix},$$

час передачі одного символу $\tau = 3$ м/сек.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$., якщо повідомлення складається з 150 символів.

Варіант 19. Взаємозв'язок джерела з приймачем описано канальною матрицею спільних ймовірностей

$$p(A,B) = \begin{Vmatrix} 0{,}10 & 0{,}10 & 0 \\ 0{,}10 & 0{,}10 & 0{,}10 \\ 0 & 0{,}20 & 0{,}30 \end{Vmatrix},$$

час передачі одного символу $\tau = 1{,}5$ м/сек.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$., якщо повідомлення складається з 250 символів.

Варіант 20. Взаємозв'язок джерела з приймачем описано канальною матрицею спільних ймовірностей

$$p(A,B) = \begin{Vmatrix} 0{,}01 & 0{,}10 & 0{,}12 & 0{,}02 \\ 0{,}02 & 0{,}10 & 0{,}05 & 0{,}07 \\ 0{,}13 & 0{,}08 & 0{,}07 & 0{,}03 \\ 0{,}02 & 0{,}03 & 0{,}06 & 0{,}09 \end{Vmatrix},$$

час передачі одного символу $\tau = 2{,}5$ м/сек.

Обчислити інформаційні характеристики дискретного каналу зв'язку, включаючи $I(a_i)$, $H(A)$, $H(B/a_i)$, $H(B/A)$,ΔI, $p(b_j)$, $H(B)$, $I(A,B)$, n, $H'(A)$, R, C, $K_э$, $R_{кр}$., якщо повідомлення складається з 350 символів.

5.3. Завдання №2. Оптимальне кодування

Для заданих повідомлень, що складають повну групу, побудувати рівномірний код і ОНК Шеннона-Фано (варіанти 1-10) або ОНК Хаффмена

(варіанти 11-20). Обчислити всі інформаційні характеристики, включаючи l_i, $l_{ср}$, H, H_{max}, μ, D, ΔD, K_c, $K_э$ побудувати кореневі дерева РБК та ОНК, оцінити оптимальність і ефективність кодів.

Вихідні дані по варіантах наведені в таблицях 5.1 і 5.2.

Ансамблі повідомлень $X = \{x_i; p(x_i)\}$ для побудови ОНК Шеннона-Фано:

Таблиця 5.1

Символ x_i	імовірності $p(x_i)$ по варіантах									
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
x_1	0,30	0,35	0,20	0,19	0,48	0,24	0,03	0,15	0,24	0,02
x_2	0,18	0,30	0,20	0,19	0,14	0,15	0,02	0,15	0,28	0,02
x_3	0,15	0,10	0,15	0,19	0,14	0,15	0,10	0,10	0,20	0,02
x_4	0,15	0,05	0,12	0,19	0,07	0,10	0,18	0,10	0,18	0,09
x_5	0,07	0,03	0,05	0,08	0,07	0,10	0,16	0,04	0,03	0,09
x_6	0,04	0,03	0,05	0,08	0,04	0,06	0,16	0,04	0,02	0,18
x_7	0,04	0,02	0,05	0,03	0,02	0,06	0,16	0,20	0,02	0,18
x_8	0,04	0,02	0,06	0,03	0,02	0,05	0,10	0,08	0,01	0,18
x_9	0,02	0,05	0,06	0,01	0,01	0,05	0,07	0,08	0,01	0,18
x_{10}	0,01	0,05	0,06	0,01	0,01	0,04	0,02	0,06	0,01	0,06

Ансамблі повідомлень $X = \{x_i; p(x_i)\}$ для побудови ОНК Хаффмена:

Таблиця 5.2

Символ x_i	імовірності $p(x_i)$ по варіантах									
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
x_1	0,02	0,01	0,25	0,30	0,06	0,01	0,04	0,06	0,02	0,04
x_2	0,02	0,01	0,23	0,30	0,06	0,19	0,05	0,18	0,03	0,15
x_3	0,03	0,02	0,15	0,10	0,06	0,01	0,05	0,09	0,02	0,04
x_4	0,07	0,02	0,15	0,10	0,05	0,19	0,06	0,18	0,01	0,15
x_5	0,18	0,07	0,06	0,03	0,05	0,03	0,06	0,09	0,01	0,10
x_6	0,16	0,07	0,05	0,03	0,05	0,19	0,10	0,18	0,01	0,06
x_7	0,13	0,07	0,05	0,02	0,12	0,03	0,10	0,02	0,18	0,10
x_8	0,13	0,14	0,02	0,02	0,15	0,19	0,14	0,18	0,20	0,20
x_9	0,15	0,14	0,02	0,05	0,20	0,08	0,14	0,02	0,24	0,08
x_{10}	0,11	0,45	0,02	0,05	0,20	0,08	0,26	0,02	0,28	0,08

5.4. Завдання №3. Завадостійке кодування

Варіант завдання визначається викладачем, або за шифром студента.

Варіант 1:

Задача 1. Згенерувати по правилах парності систематичний коригуючий код Хеммінга для бінарного слова **100011100110**

Задача 2. Виконати діагностику, корекцію і декодування циклічного коригуючого коду (16;7) **0000111010001110** за допомогою породжуючого поліному $g(x)=x^9+x^8+x+1.$

Варіант 2.

Задача 1. Виконати діагностику, корекцію, декодування циклічного коригуючого коду (16;7) **1101011010010110** за допомогою породжуючого поліному $g(x)=x^9+x^8+x+1.$

Задача 2. Згенерувати систематичний коригуючий код Хеммінга для бінарного слова **000101100111** за допомогою породжуючої матриці.

Варіант 3.

Задача 1. Виконати діагностику, корекцію і декодування систематичного коригуючого коду Хеммінга **000110100010010000** за допомогою правил парності.

Задача 2. Згенерувати циклічний коригуючий код (16;7) за допомогою породжуючого поліному $g(x)=x^9+x^8+x+1$. За початкове двійкове слово вибрати букву імені в системі ISO – 7bit.

Варіант 4.

Задача 1. Згенерувати коригуючий мажоритарний код 5 - подвоєння для 7-бітового слова, ісходник вибрати самостійно. Ефективність коригуючого мажоритарного коду. Привести приклади діагностики помилок.

Задача 2. Виконати діагностику, корекцію і декодування коригуючого циклічного коду (16;7) **1001111010001110** за допомогою породжуючого поліному $g(x)=x^9+x^8+x+1.$

Варіант 5.

Задача 1. Виконати діагностику, корекцію і декодування коригуючого циклічного коду (16;7) **1001111010010110** за допомогою породжуючого поліному $g(x)=x^9+x^8+x+1.$

Задача 2. Згенерувати коригуючий мажоритарний код 3-удвоения для 7-бітового слова. Ісходник вибрати самостійно. Привести приклади діагностики помилок в інформаційній і контрольній частинах коду.

Варіант 6.

Задача 1. Виконати за допомогою породжуючої матриці діагностику систематичного коригуючого коду Хеммінга **00111011001001000.**

Виконати корекцію і декодування коду.

Задача 2. За допомогою породжуючого поліному $g(x)= x^9 + x^8 + x + 1.$

виконати діагностику коригую чого циклічного коду (16:7) **1001110010011000**.

Скоректувати помилку і декодувати циклічний код

Варіант 7.

Задача 1. Згенерувати систематичний коригуючий код Хеммінга по правилах парності. Початкове двійкове 12-бітове слово вибрати самостійно.

Задача 2. За допомогою породжуючого поліному $g(x)= x^9 + x^8 + x + 1.$ виконати діагностику коригуючого циклічного коду **1001000010011000.**

Виконати корекцію і декодування.

Варіант 8.

Задача 1. Виконати діагностику, корекцію і декодування коригуючого циклічного коду (16;7) **1001010010010101** за допомогою породжуючого полінома $g(x)= x^9 + x^8 + x + 1.$

Задача 2. Згенерувати систематичний коригуючий код Хеммінга для 12 бітового слова за допомогою правил парності.

Варіант 9.

Задача 1. Виконати діагностику, корекцію, декодування коригуючого циклічного коду **1000011010001110** за допомогою породжуючого полінома $g(x)= x^9 + x^8 + x + 1.$

Задача 2. Згенерувати коригуючий систематичний код Хеммінга за допомогою породжуючої матриці. За ісходник прийняти першу букву прізвища в ISO-7bit.

Варіант 10.

Задача 1. За допомогою породжуючого полінома $g(x)= x^9 + x^8 + x + 1.$ виконати діагностику, корекцію, і декодування коригуючого циклічного коду **1001010010010000.**

Задача 2. Згенерувати коригуючий систематичний код Хеммінга за допомогою породжуючої матриці. За ісходник прийняти першу букву прізвища в ISO-7bit. Ефективність коду.

Варіант 11.

Задача 1. Згенерувати коригуючий циклічний код за допомогою породжуючої матриці G (7;16). За ісходник прийняти першу букву прізвища в ISO-7bit

Задача 2. Виконати діагностику, корекцію, декодування коригуючого систематичного коду Хеммінга **0010000110100100000** за допомогою породжуючої матриці.

Варіант 12.

Задача 1. Згенерувати коригуючий циклічний код (16;7). За початкове двійкове слово вибрати букву імені в системі ISO - 7bit, породжуючий поліном

$g(x)=x^9+x^8+x+1.$

Задача 2. Виконати діагностику, корекцію, декодування коригуючого систематичного коду Хеммінга **00111011001001000** за допомогою породжуючої матриці.

Варіант 13.

Задача 1. Згенерувати коригуючий циклічний код (16;7). За початкове двійкове слово вибрати букву імені в системі ISO - 7bit, породжуючий поліном $g(x)=x^9+x^8+x+1.$ Ефективність коду.

Задача 2. Виконати діагностику, корекцію і декодування коригуючого систематичного коду Хеммінга **00111010101001000** за допомогою правил парності.

Варіант 14.

Задача 1. Виконати діагностику, корекцію і декодування коригуючого систематичного коду Хеммінга **00111010011001000** за допомогою правил парності.

Задача 2. Згенерувати коригуючий циклічний код (16;7). За початкове двійкове слово вибрати букву імені в системі ISO - 7bit, породжуючий поліном $g(x)=x^9+x^8+x+1.$

Варіант 15.

Задача 1. За допомогою породжуючого поліному $g(x)=x^9+x^8+x+1$ згенерувати коригуючий циклічний код (16;7), за початкове двійкове слово вибрати букву імені в системі ISO - 7bit. Ефективність коду.

Задача 2. Виконати діагностику, корекцію і декодування систематичного коригуючого коду Хеммінга **10101000100011011** за допомогою правил парності.

Варіант 16.

Задача 1. Виконати діагностику, корекцію і декодування систематичного коригуючого коду Хеммінга **00111010001101000** за допомогою правил парності.

Задача 2. Згенерувати коригуючий циклічний код (16;7) за допомогою породжуючої матриці G (7;16). За ісходник прийняти першу букву прізвища в ISO-7bit.

Варіант 17.

Задача 1. Виконати за допомогою породжуючої матриці діагностику систематичного коригую чого коду Хеммінга **10101000100111111.** Виконати корекцію і декодування коду.

Задача 2. За допомогою породжуючого поліному $g(x)=x^9+x^8+x+1.$ згенерувати коригуючий циклічний код (16;7). За ісходник прийняти початкову букву прізвища в системі ISO - 7bit Ефективність коду.

Варіант 18.

Задача 1. Виконати діагностику, корекцію і декодування систематичного коригуючого коду Хеммінга **00111010001001010** за допомогою правил парності.

Задача 2. Згенерувати коригуючий циклічний код за допомогою породжуючої матриці G (7;16). За ісходник прийняти початкову букву прізвища в ISO-7bit. Ефективність коду.

Варіант 19.

Задача 1. Згенерувати за допомогою породжуючої матриці систематичний коригуючий код Хеммінга, за ісходник прийняти початкову букву прізвища в ISO-7bit.

Задача 2. Виконати діагностику коригуючого мажоритарного коду 3-удвоения **101010100001011010001** скоректувати і декодувати код. Ефективність коду.

Варіант 20.

Задача 1. Згенерувати систематичний коригуючий код Хеммінга по правилах парності. За ісходник прийняти початкову букву прізвища в ISO-7bit.

Задача 2. За допомогою породжуючого поліному $g(x)=x^9+x^8+x+1$ виконати діагностику коригуючого циклічного коду **1101000010010000,** виконати корекцію і декодування коду.

Література

1. Цимбал В. Л. Теорія інформації й кодування. 4-і вид. - К.: Вища школа, 1992 – 263 с.
2. Жураковський Ю. П., Полтарак В. П. Теорія інформації та кодування – К.: Вища Школа, 2001 – 255 с.
3. КРАП О. К. Теорія інформації та кодування. Методичні вказівки та контрольні завдання до практичних занять - Одеса ОНМУ 2006 – 63с.
4. Дейт К. Введення в системи баз даних. Пер. с англ. 6-і вид. – К.: Діалектика, 1998.
5. Бэрри Нанс. Комп'ютерні мережі. Пер. с англ. – М.: Біном, 1996.
6. Фигурнов В. Э. IBM PC для користувача. 7-і вид. – М.: ИНФРА, 1998.
7. Теорія й практика забезпечення інформаційної безпеки. Під ред. Зегжди П.Д. – М.: Яхтемен, 1996.
8. Колесник В. Д., Полтырев Г. Ш. Курс теории информации. – М. Наука., 1982 – 416 с.
9. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М. ДМК. 2002 – 448 с.
10. Новиков Ф. А. Дискретная математика для программистов. – СПб. Питер. 2000 – 304 с.

ДОДАТКИ

Додаток 1

Таблиця двійкових логарифмів цілих чисел

x	*log x*	*x*	*log x*	*x*	*log x*
1	0,00000	38	5,24793	75	6,22882
2	1,00000	39	5,28540	76	6,24793
3	1,58496	40	5,32193	77	6,26679
4	2,00000	41	5,35755	78	6,28540
5	2,32193	42	5,39232	79	6,30378
6	2,58496	43	5,42626	80	6,32193
7	2,80735	44	5,45943	81	6,33985
8	3,00000	45	5,49185	82	6,35755
9	3,16993	46	5,52356	83	6,37504
10	3,32193	47	5,55459	84	6,39232
11	3,45943	48	5,58496	85	6,40939
12	3,58496	49	5,61471	86	6,42626
13	3,70044	50	5,64386	87	6,44294
14	3,80735	51	5,67242	88	6,45943
15	3,90689	52	5,70044	89	6,47573
16	4,00000	53	5,72792	90	6,49185
17	4,08746	54	5,75489	91	6,50779
18	4,16993	55	5,78136	92	6,52356
19	4,24793	56	5,80735	93	6,53916
20	4,32193	57	5,83289	94	6,55459
21	4,39232	58	5,85798	95	6,56986
22	4,45943	59	5,88264	96	6,58496
23	4.52356	60	5,90689	97	6,59991
24	4,58496	61	5,93074	98	6,61471
25	4,64386	62	5,95420	99	6,62936
26	4,70044	63	5,97728	100	6,64386
27	4,75489	64	6,00000	200	7,644
28	4,80735	65	6,02237	300	8,229
29	4,85798	66	6,04439	400	8,614
30	4,90689	67	6,06609	500	8,966
31	4,95420	68	6,08746	600	9,229
32	5,00000	69	6,10852	700	9,451
33	5,04439	70	6,12928	800	9,644
34	5,08746	71	6,14975	900	9,814
35	5,12928	72	6,16992	1000	9,965
36	5,16993	73	6.18982	10000	13,288
37	5,20945	74	6,20945		

Додаток 2

Таблиця значень ентропії $- p_i \log p_i$

p_i	$- p_i \log p_i$	p_i	$- p_i \log p_i$	p_i	$- p_i \log p_i$
0,00	0,0000				
0,01	0,0664	0,36	0,5306	0,71	0,3508
0,02	0,1129	0,37	0,5307	0,72	0,3412
0,03	0,1517	0,38	0,5304	0,73	0,3314
0,04	0,1857	0,39	0,5298	0,74	0,3215
0,05	0,2161	0,40	0,5288	0,75	0,3113
0,06	0,2435	0,41	0,5274	0,76	0,3009
0,07	0,2686	0,42	0,5256	0,77	0,2903
0,08	0,2915	0,43	0,5236	0,78	0,2796
0,09	0,3127	0,44	0,5211	0,79	0,2687
0,10	0,3322	0,45	0,5184	0,80	0,2575
0,11	0,3503	0,46	0,5153	0,81	0,2462
0,12	0,3671	0,47	0,5120	0,82	0,2348
0,13	0,3826	0,48	0,5083	0,83	0,2231
0,14	0,3971	0,49	0,5043	0,84	0,2113
0,15	0,4105	0,50	0,5000	0,85	0,1993
0,16	0,4230	0,51	0,4954	0,86	0,1871
0,17	0,4346	0,52	0,4906	0,87	0,1748
0,18	0,4453	0,53	0,4854	0,88	0,1623
0,19	0,4552	0,54	0,4800	0,89	0,1496
0,20	0,4644	0,55	0,4744	0,90	0,1368
0,21	0,4728	0,56	0,4684	0,91	0,1238
0,22	0,4806	0,57	0,4623	0,92	0,1106
0,23	0,4877	0,58	0,4558	0,93	0,0974
0,24	0,4941	0,59	0,4491	0,94	0,0839
0,25	0,5000	0,60	0,4422	0,95	0,0703
0,26	0,5053	0,61	0,4350	0,96	0,0565
0,27	0,5100	0,62	0,4276	0,97	0,0426
0,28	0,5142	0,63	0,4199	0,98	0,0286
0,29	0,5179	0,64	0,4121	0,99	0,0140
0,30	0,5211	0,65	0,4040		
0,31	0,5238	0,66	0,3957		
0,32	0,5260	0,67	0,3871		
0,33	0,5278	0,68	0,3784		
0,34	0,5292	0,69	0,3694		
0,35	0,5301	0,70	0,3602		

Додаток 3

Коригуючий систематичний код Хемминга

Таблиця 1

n	$n_и$	$n_к$	n	$n_и$	$n_к$
1	0	1	9	5	4
2	0	2	10	6	4
3	1	2	11	7	4
4	1	3	12	8	4
5	2	3	13	9	4
6	3	3	14	10	4
7	4	3	15	11	4
8	4	4	16	11	5

Таблиця 2

n	Двійковий код	Перевірочні коефіцієнти	n	Двійковий код	Перевірочні коефіцієнти
1	0 0 0 1	a_1	7	0 1 1 1	a_7
2	0 0 1 0	a_2	8	1 0 0 0	a_8
3	0 0 1 1	a_3	9	1 0 0 1	a_9
4	0 1 0 0	a_4	10	1 0 1 0	a_{10}
5	0 1 0 1	a_5	11	1 0 1 1	a_{11}
6	0 1 1 0	a_6			

Таблиця 3

№ перевірки	Перевірочні позиції	№ контрольного символу
1	1, 3, 5, 7, 9, 11, …	1
2	2, 3, 6, 7, 10, 11, 14, 15, 18, 19, 22, 23, 26, 27, 30, 31, …	2
3	4, 5, 6, 7, 12, 13, 14, 15, 20, 21, 22, 23, 28, 29, 30, 31, …	3
4	8, 9, 10, 11, 12, 13, 14, 15, 24, 25, 26, 27, 28, 29, 30, 31, …	4

Додаток 4

Стандартний телеграфний код №3

Значення кодової комбінації		Кодова комбінація
на першому регістрі	на другому регістрі	
А	—	0011010
Б	?	0011001
В	:	1001100
Г	Хто там?	0011100
Д	З	0111000
Е,Ё	%	0010011
Ж		1100001
З		1010010
И	8	1110000
К	Дзвоник	0100011
Л	(	0001011
М	)	1100010
Н	.	1010001
О	,	1010100
П	9	1000110
Р	0	1001010
С	1	0001101
Т	4	1100100
У	Апостроф	0101010
Ф	5	1000101
Х	7	0110010
Ц	=	1001001
Щ	2	0100111
Ь	/	0010110
Ы	6	0010101
Я	+	0110001
Повернення каретки		1000011
Переклад рядка		1011000
Букви		0001110
Цифри		0100110
Пробіл		1101000
Неперфорована стрічка		0000111
Сигнал перепопиту		0110100
α		0101001
β		0101100

Додаток 5

Розподіл ймовірностей букв у російських текстах

Буква	Середня імовірність появи у тексті	$- p_i \log_2 p_i$	Буква	Середня імовірність появи у тексті	$- p_i \log_2 p_i$
пробіл	0,175	0,440	Я	0,018	0,104
О	0,090	0,313	Ы	0,016	0,095
Е,Ё	0,072	0,273	З	0,016	0,095
А	0,062	0,249	Ъ,Ь	0,014	0,086
И	0,062	0,248	Б	0,014	0,086
Н	0,053	0,238	Г	0,013	0,081
Т	0,053	0,225	Ч	0,012	0,076
С	0,045	0,201	Й	0,010	0,066
Р	0,040	0,185	Х	0,009	0,061
В	0,038	0,179	Ж	0,007	0,050
Л	0,035	0,169	Ю	0,006	0,044
К	0,028	0,144	Ш	0,006	0,044
М	0,026	0,136	Ц	0,004	0,031
Д	0,025	0,133	Щ	0,003	0,025
П	0,023	0,125	Э	0,003	0,025
У	0,021	0,117	Ф	0,002	0,018

Примітка. Для російського алфавіту, з урахуванням пробілу, а також з обліком нерівно ймовірностей, появи символів H_1 = 4,35 біт/символ, з урахуванням двобуквених сполучень H_2 = 3,52 біт/символ; з обліком трибуквених H_3 = 3,01 біт/символ.

Додаток 6

Розподіл ймовірностей букв в українських текстах

(без обліку імовірності появи в текстах пробілу між словами)

Буква	Середня імовірність появи в тексті	$-p_i \log_2 p_i$	Буква	Середня імовірність появи в тексті	$-p_i \log_2 p_i$
А	0,0855	0,303348	Н	0,0613	0,247431
Б	0,0183	0,105195	О	0,1037	0,33 8683
В	0,0540	0,227388	П	0,0296	0,150316
Г	0,0150	0,090883	Р	0,0468	0,206732
Д	0,0298	0,151043	С	0,0394	0,183827
Е	0,0473	0,208511	Т	0,0509	0,218961
Є	0,0036	0,029224	У	0,03689	0,175321
Ж	0,0080	0,055726	Ф	0,0023	0,020158
З	0,0203	0,113716	Х	0,0097	0,064872
І	0,0684	0,264941	Ц	0,0074	0,052379
И	0,0634	0,252546	Ч	0,0136	0,084323
Ї	0,0067	0,048385	Ш	0,0110	0,071570
Й	0,0202	0,113716	Щ	0,0091	0,061697
К	0,0368	0,175321	Ю	0,0072	0,051248
Л	0,0388	0,179933	Я	0,0172	0,100817
М	0,0268	0,139939	Ь	0,0246	0,89029

Примітка. Для українського алфавіту H=4,577179 біт/символ.

Додаток 7

Розподіл ймовірностей букв в англійському тексті

Буква	Середня імовірність появи в тексті	$-p_i \log_2 p_i$	Буква	Середня імовірність появи в тексті	$-p_i \log_2 p_i$
A	0,063	0,251	N	,059	0,241
B	0,11	0,072	O	0,065	0,256
C	0,023	0,125	P	0,018	0,104
D	0,035	0,169	Q	0,001	0,009
E	0,105	0,341	R	0,054	0,227
F	0,028	0,125	S	0,052	0,222
G	0,11	0,072	T	0,72	0,273
H	0,047	0,207	U	0,023	0,125
I	0,055	0,230	V	0,008	0,072
J	0,001	0,009	W	0,012	0,076
K	0,003	0,061	X	0,001	0,025
L	0,029	0,148	Y	0,012	0,076
M	0,021	0,117	Z	0,001	0,009
			(пробіл)	0,2	0,464

Примітка. Для англійського алфавіту H_{max} =4,754 біт/символ, нерівноімовірних взаємонезалежних символів H = 4,043 біт/символ; з урахуванням двобуквених сполучень — 3,32 біт/символ, трибуквених — 3,10 біт/символ; п′ятилітерних 12біт/символ, восьми літерних сполук 1,86 біт/символ.

Без обліку пробілу H_{max} = 4,7 біт/символ, для нерівноімовірних взаємонезалежних символів H = 4,14 біт/символ; для двобуквених сполучень — 3,56 біт/символ, трибуквених — 3,32 біт/символ; п’ятилітерних 2,6біт\символ, восьми літерних сполучень 2,3 біт/символ.