В роботі запропонована система передавання даних, шифрованих псевдовипадковими послідовностями та показано принцип її роботи на прикладі 64-бітного інформаційного повідомлення. Досліджено вплив канального кодування на тривалість часу синхронізації в залежності від відносного рівня шуму в каналі зв'язку для різних значень кількості бітів парності канального кодера

Ключові слова: логістичне відображення, канальне колування, передавання даних, коди Хеммінга

В работе предложена система передачи данных, шифрованных псевдослучайными последовательностями и показан принцип ее работы на примере 64-битного информационного сообщения. Исследовано влияние канального кодирования на время синхронизации в зависимости от относительного уровня шума в канале связи для различных значений количества битов четности канального кодера

Ключевые слова: логистическое отображение, канальное кодирование, передача данных, коды Хемминга

УДК 621.391

КОДУВАННЯ КАНАЛУ ПЕРЕДАВАННЯ ДАНИХ, ШИФРОВАНИХ ПСЕВДОВИПАДКОВИМИ ПОСЛІДОВНОСТЯМИ

Р.Л. Політанський
Кандидат фізико-математичних наук, доцент*
Контактний тел.: (03722) 4-24-36
E-mail: polroos@mail.ru
Л.Ф. Політанський
Доктор технічних наук, професор, завідувач кафедри*
Контактний тел.: (03722) 4-24-36
П.М. Шпатар
Кандидат технічних наук, доцент*
Контактний тел.: (03722) 4-24-36
П.В. Іванюк
Аспірант*
Контактний тел.: 066-940-71-57
E-mail: ivanyukpetro@gmail.com
*Кафедра радіотехніки та інформаційної безпеки
Чернівецький національний університет
ім. Юрія Федьковича
вул. Сторожинецька, 101, м. Чернівці, Україна, 58000

1. Вступ

Перспективним напрямком розвитку засобів зв'язку є використання широкосмугових систем, що використовують великі ансамблі малокорельованих між собою сигналів, формування яких здійснюється, зокрема, на основі псевдовипадкових послідовностей. При цьому актуальним є питання впливу завад у каналі зв'язку на синхронізацію приймальної та передавальної частин системи, проблемам якої присвячені актуальні роботи вітчизняних та зарубіжних авторів [1-5]. Можна очікувати, що оброблення синхроімпульсів канальними кодерами, крім енергетичного виграшу кодування, підвищення швидкості передавання даних, зменшення ширини смуги пропускання, обумовлюватиме зменшення тривалості часу синхронізації, оскільки при цьому ймовірність помилкових канальних бітів падає.

Метою даної роботи є дослідження впливу шумів в каналі зв'язку на тривалість процесу синхронізації передавальної та приймальної частини запропонованої системи зв'язку.

2. Генерування псевдовипадкових бінарних послідовностей

Сигнали, генеровані нелінійними динамічними системами, є новим класом псевдовипадкових сигналів [6]. Найбільш важливим завданням для формування неперіодичної псевдовипадкової послідовності є розроблення алгоритмів кодування бітів наборами символів, що не повторюються в часі.

В роботі для генерування псевдовипадкових послідовностей використовувалося одномірне дискретне хаотичне відображення наступного вигляду:

$$x_{n+1} = 4x_n(1-x_n),$$

де $n = 0,1,2,3...$; x_0 – початковий елемент послідовності, що вибирається з інтервалу дійсних чисел $(0;1)$.

Кожній ітерації логістичного відображення ставиться у відповідність біт за наступним законом:

$$b_n = \begin{cases} 0, \text{ якщо } x_n \in \left(0;\frac{1}{2}\right] \\ 1, \text{ якщо } x_n \in \left(\frac{1}{2};1\right] \end{cases}.$$

Отримані таким чином хаотичні псевдовипадкові бінарні послідовності $B(x) = \{b_1(x_1), b_2(x_2), ..., b_n(x_n)\}$ використовувалися для шифрування інформаційних повідомлень в запропонованій системі зв'язку, структурна схема якої приведена на рис. 1.

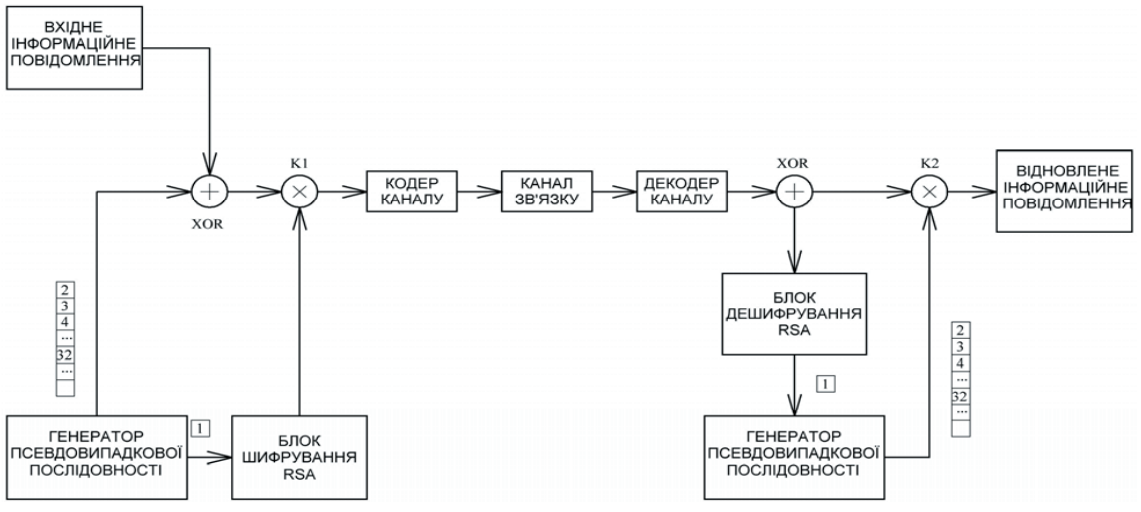

Рис. 1. Структурна схема системи зв'язку з шифруванням даних псевдовипадковими послідовностями

3. Приклад системи зв'язку

Розглянемо принцип роботи запропонованої схеми системи зв'язку на прикладі 64-бітової інформаційної послідовності.

В приведеній системі шифрування інформації розпочинається із генерування псевдовипадкової послідовності чисел. За цифровим значенням першого члена псевдовипадкової послідовності формується 64-бітовий ключ, що шифрується за допомогою криптосистеми RSA (при цьому використовується відкритий ключ того, хто отримує повідомлення) з наступним передаванням на блок конкатенації сигналів K1. Наступні 64 значення послідовності формують 64-бітовий ключ-сеансу, що використовується для шифрування інформаційного повідомлення. Шифрування вхідного інформаційного повідомлення із ключем сеансу відбувається за допомогою операції XOR. Зашифровані таким чином 64 біти повідомлення приєднуються до 64-бітового ключа, зашифрованого RSA. Утворена таким чином 128-бітова послідовність кодується кодером каналу і передається в канал зв'язку. Канальне кодування використовується для підвищення якості зв'язку.

В якості кодера каналу зв'язку можуть використовуватися кодери, що формують коди Хеммінга, коди Боуза-Чоуході-Хоквенгема (БЧХ), коди Голея та інші.

Після процесу декодування послідовності приймальною стороною здійснюється її розділення на 2 блоки по 64 біти в блоці розділення сигналів K2. За допомогою першого блоку, дешифрованого алгоритмом RSA (при цьому використовується закритий ключ одержувача повідомлення), здійснюється запуск генератора, що формує 64-бітовий ключ, аналогічний ключу-сеансу передавальної сторони. За допомогою сформованого ключа-сеансу здійснюється однозначне дешифрування другого 64-бітового блоку операцією XOR. Таким чином отримуємо відновлену 64-бітову інформаційну послідовність.

4. Дослідження впливу канального кодування на час синхронізації

Оброблення інформаційного повідомлення лінійними блоковими кодерами обумовлює зміну часових характеристик двійкових імпульсів цифрового сигналу (рис. 2).

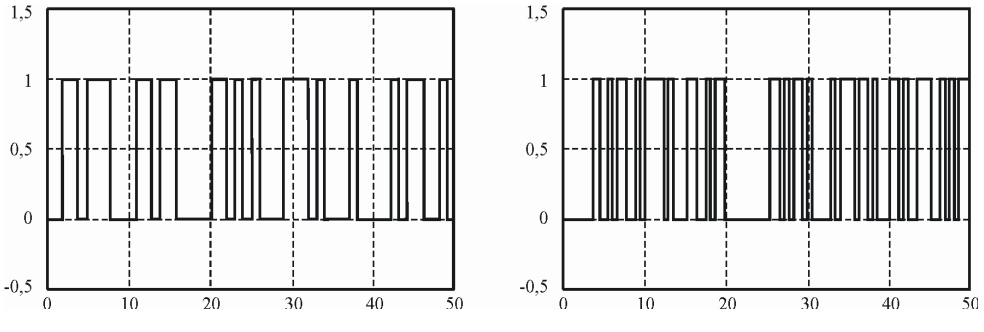

Рис. 2. Часові діаграми сигналу на вході та виході блокового кодера Хеммінга (7, 4) (а) та (б) відповідно

Тривалість бітової послідовності T , включає в себе тривалість інформаційної T_i та синхронізуючої послідовностей T_c (рис. 3).

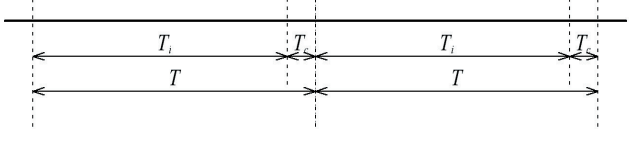

Рис. 3. Часова діаграма передавання синхроімпульсів та інформаційного повідомлення

Моделювання роботи запропонованої схеми здійснювалося в програмному середовищі Matlab. Шифрування інформаційного сигналу псевдовипадковими послідовностями не впливає на роботу лінійного блокового кодера та не збільшує ймовірність виникнення помилкового біту [7, 8].

Проведений аналіз процесу синхронізації за запропонованою схемою вказує на доцільність кодування послідовності синхронізації. Збільшення довжини кодового слова не суттєво впливає на час передавання бітів у випадку, якщо вона є набагато меншою в порівнянні з послідовністю даних, що передаються по каналу зв'язку.

При дослідженні впливу шумів в каналі зв'язку на час синхронізації для різних кодів вважалося, що час синхронізації дорівнює часу передавання мінімальної кількості імпульсів, що забезпечує ідентифікацію та визначення значення параметру x_0.

Для забезпечення синхронної роботи кількість імпульсів повинна збільшуватися на кількість бітів, спотворених в каналі зв'язку внаслідок дії імпульсних завад.

При бінарній фазовій модуляції ймовірність помилки канального біту визначається наступним виразом [9]:

$$p = Q\left(\sqrt{2\frac{E_b}{N_0}}\right),$$

де Q – інтеграл помилок $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{u^2}{2}}du$;

E_b – енергія біту інформації;

N_0 – спектральна густина потужності шуму в каналі.

При цьому середня кількість помилкових бітів у послідовності синхронізації довжиною N біт дорівнюватиме:

$$n_i = Np.$$

Отже, необхідна кількість імпульсів у послідовності синхронізації згідно запропонованої моделі становитиме:

$$\tilde{N} = N(1+p).$$

При канальному кодуванні кодом (n,k) ймовірність помилки дорівнюватиме:

$$p_c = Q\left(\sqrt{2\frac{k}{n}\frac{E_A}{N_0}}\right).$$

При цьому ймовірність неправильно декодованого біту становить:

$$P_B = \frac{1}{n}\sum_{j=t+1}^{n} C_n^j p_c^j (1-p_c)^{n-j}.$$

Таким чином, довжина закодованої лінійним блоковим кодером (n,k) послідовності синхронізації та середня кількість помилкових бітів у ній відповідно дорівнюватиме:

$$N_c = N\frac{n}{k},$$

$$n_{ic} = N_c P_B = N\frac{n}{k}P_B.$$

Вплив шумів у каналі зв'язку на час синхронізації досліджувався при швидкості передавання бітів $R = 10$ Мбіт/с.

Тривалість передавання незакодованої та закодованої послідовності синхроімпульсів визначається наступними формулами:

$$T_{0n} = \frac{\tilde{N}}{R} = N\frac{1+P_B}{R},$$

$$T_n = \frac{\tilde{N}_c}{R_c} = \frac{N\frac{n}{k}(1+P_B)}{R\frac{n}{k}} = N\frac{1+P_B}{R}.$$

На рис. 4 та рис. 5 приведені залежності тривалості часу синхронізації від відносного рівня шуму для кодів Хеммінга різної довжини і різних видів кодів БЧХ та коду Голея відповідно. При розрахунках в якості характеристики каналу зв'язку використовувався відносний рівень шуму, що дорівнює квадратному кореню із відношення спектру потужності шуму до енергії біту:

$$\eta = \sqrt{\frac{N_0}{E_b}}.$$

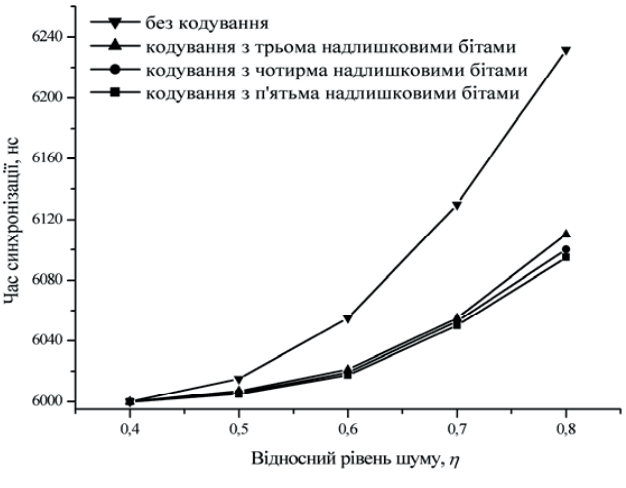

Рис. 4. Залежність часу синхронізації від вісного рівня шуму для кодів Хеммінга різної довжини

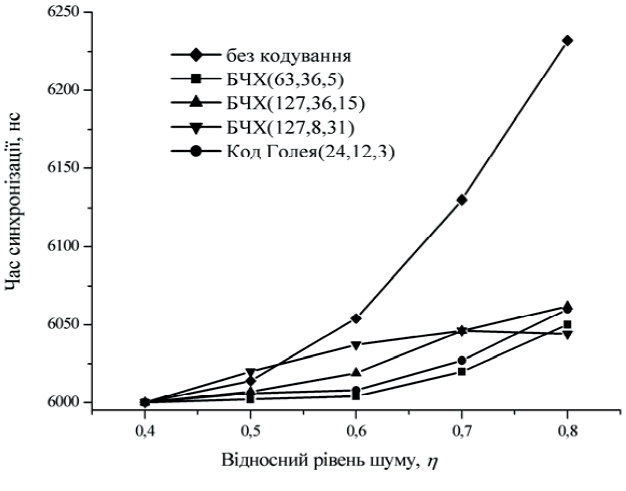

Рис. 5. Залежність часу синхронізації від відносного рівня шуму для різних кодів БЧХ та коду Голея

З отриманих результатів випливає, що більш потужні коди БЧХ суттєво зменшують тривалість часу синхронізації у порівнянні з кодами Хеммінга.

Для запропонованої системи спостерігається суттєвий вплив шумів в каналі зв'язку на час синхронізації при значенні η більше 0.4, тоді як в роботі [5] це значення становить 0.3.

Таким чином, використання відносно простих схем лінійного блокового кодування призводить до зменшення часу синхронізації на рівні 50÷100 нс при значеннях η, що знаходиться у межах від 0.4 до 0.8 для швидкості передавання бітів R=10 Мбіт/с.

При використанні кодів БЧХ та кодів Голея зменшення тривалості синхронізації спостерігається на рівні 100÷200 нс.

5. Результати роботи та висновки

1. Запропонована система передавання даних, шифрованих псевдовипадковими послідовностями, забезпечує крипостійкість, що визначається розрядністю значення параметра генерування x_0 та використанням алгоритму RSA.

2. На основі запропонованої моделі кількісної оцінки знайдені залежності тривалості часу синхронізації від відносного рівня шуму в каналі зв'язку для різних значень кількості бітів парності канального кодера. Використання відносно простих схем лінійного блокового кодування зменшує час синхронізації на 50÷100 нс при відносному рівні шуму $\eta = 0.4 \pm 0.8$ при швидкості передавання 10 Мбіт/с.

3. Використання лінійних блокових кодів забезпечує більшу стійкість процесу синхронізації до впливу шумів в каналі зв'язку.

Література

1. Пиковский, А. Синхронизация. Фундаментальное нелинейное явление [Текст] / А. Пиковский, М. Розенблюм, Ю. Куртс. – М.: Техносфера, 2003. – 510 с.
2. Дмитриев, А.С. Динамический хаос: новые носители информации для систем связи [Текст] / А.С. Дмитриев, А.И. Панас. – М.: Издательство физико-математической литературы, 2002. – 252 с.
3. Кальянов, Г.И. Шифрование цифровой информации при использовании генераторов с хаотической динамикой [Текст] / Г.И. Кальянов, Э.В. Кальянов // Радиотехника и электроника. – 2008. – Т. 53, № 4. – С. 459–467.
4. Дмитриев, А.С. Передача информации с использованием синхронного хаотического отклика при наличии фильтрации в канале связи [Текст] / А.С. Дмитриев, Л.В. Кузьмин // Письма в ЖТФ. – 1999. – Т. 25, № 16. – С. 71–77.
5. Andreyev Yu. V. CDMA communications using maps with stored information [Текст] / Yu. V. Andreyev, A. S. Dmitriev, D. A. Kuminov, S. O. Starkov // European Conference on Circuit Theory and Design. – Budapest.– 1997. – P. 324–329.
6. Кислов, В.Я. Применение хаотических сигналов в информационных технологиях [Текст] / В.Я. Кислов, В.В. Колесов, Р.В. Беляев // Радиоэлектроника. Наносистемы. Информационные технологии. – 2009. – Т.1, №1-2. С. 23–32.
7. Політанський, Р.Л. Система передавання даних з використанням генераторів хаосу [Текст] / Р.Л. Політанський, Л.Ф. Політанський, О.В. Гресь, С.Д. Галюк // Всеукраинский межведомственный научно-технический сборник. – Харків, 2011.– № 164: Радиотехника. – С. 66–71.
8. Політанський, Р.Л. Властивості псевдовипадкових послідовностей, генерованих картами хаосу [Текст] / Р.Л. Політанський, З.Ю. Готра // Збірник наукових праць «Комп'ютерні технології друкарства». – Львів, 2010. – С. 97–105.
9. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Текст] / Б. Скляр. – М.: «Издательский дом Вильямс», 2007. – 1104 с.

Abstract

This paper presents a system of data transmission encrypted by pseudo-random sequences and shows its work principle by the example of 64-bit data message. One-dimensional discrete map that always generates non-repetitious sequence of numbers depending on initial conditions was used as a generator of pseudo-random sequences. The model of quantitative assessment of noise impact in communication channel on duration time of synchronization period according to the number of excess bits in a code word is proposed. The impact of channel coding on duration time of synchronization period depending on the relative amount of noise in communication channel for various numbers of bits of channel encoder parity is examined. It is shown that the usage of relatively simple linear block coding schemes (Hamming codes) results in reduction of duration time of synchronization period at a rate of 50÷100ns with the relative amount of noise 0.4÷0.8 for bit rate R=10 Mbit/s, and the usage of BCH codes and Golay codes results in reduction of duration time of synchronization period at a rate of 100÷200ns

Keywords*: logistic map, channel coding, data transmission, Hamming codes*