УДК 681.324:621.325

М.І. Науменко[1], І.Є.Кужель[2]

[1]*Департамент військової освіти та науки МО України, Київ*
[2]*Харківський університет Повітряних Сил ім. І. Кожедуба, Харків*

ДОСЛІДЖЕННЯ ВІРОГІДНОСТІ ПЕРЕДАЧІ ДАНИХ ПРИ ВИКОРИСТАННІ ПОТОКОВИХ ТЕОРЕТИКО-КОДОВИХ СХЕМ

Проведений розрахунок показників вірогідності передачі інформації в каналах з помилками , що групуються на основі використання математичної моделі Бенета-Фройліха. Дана оцінка енергетичного виграшу від застосування запропонованих теоретико-кодових схем в каналах передачі даних з незалежними помилками та помилками, що групуються. Розглянуті залежності ймовірності помилкового прийому символу в теоретико-кодовій схемі з алгебраїчними згортальними кодами. Проведений аналіз застосування алгебраїчних згортальних кодів в потоковій теоретико-кодовій схемі.

Ключові слова: *завадостійке кодування , теоретико-кодові схеми, пакет помилок, ймовірність, модель.*

Вступ

Основним і найбільш ефективним засобом підвищення вірогідності даних, що передаються є методи завадостійкого кодування [1 – 3, 6, 7, 9]. Перспективним напрямком в їх розвитку є згортальні коди, які дозволяють, за інших рівних умов, отримати більший енергетичний виграш від кодування [5].

Одним із засобів інтегрованого забезпечення вірогідності та інформаційної таємності є теоретико-кодові схеми, побудовані з використанням алгебраїчних блокових кодів [9]. Їх застосування дозволяє сумістити завадостійке кодування із спеціальним перетворенням даних і, таким чином, забезпечити необхідну вірогідність та інформаційну таємність з меншими витратами. У той же час відомо, що потокова (безперервна) обробка даних, які передаються ефективніша як при завадостійкому кодуванні, так і при реалізації механізмів захисту інформації від розкриття супротивником її змісту [4, 8].

Таким чином, **актуальним напрямком** досліджень є розробка потокових методів обробки даних, що передаються, які дозволяють інтегровано підвищувати вірогідність інформації в АСУВ та її інформаційну таємність.

Мета статті: проведення розрахунку показників вірогідності передачі інформації в каналах з помилками , що групуються на основі використання математичної моделі Бенета-Фройліха

Результати теоретичних досліджень

Зручним інструментом для розрахунку показників вірогідності передачі інформації в каналах з помилками, що групуються, є математична модель Бенета-Фройліха, в якій не накладається обмеження на вигляд закону розподілу довжин пакетів помилок [6]. У роботі [7] запропонована методика оцінки ЕВК в каналах, що описується спрощеною моделлю Бенета-Фройліха.

Спрощена модель Бенета-Фройліха описується наступними допущеннями і показниками:

– помилки можуть виникати тільки в межах пакету помилок з постійною ймовірністю $P_\varepsilon = 1$ (суцільні пакети);

– примикання і взаємне перекриття суцільних пакетів відсутні;

– постійна ймовірність $P_п$ – ймовірність того, що з даної позиції почнеться суцільний пакет помилок будь-якої довжини;

– $P(\ell)$ – ймовірність виникнення суцільного пакету довжини ℓ ;

– $P_п(\ell)$ – ймовірність того, що з даної позиції почнеться суцільний пакет помилок довжини ℓ $P_п(\ell) = P_п \cdot P(\ell)$.

Для завдання спрощеної моделі Бенета-Фройліха досить задати ймовірність $P_п$ і розподіл $P(\ell)$. Значення ймовірності $P_п$ і розподіл $P(\ell)$ можна набути експериментально на достатньо великому об'ємі вибірки [6].

Розподіл $P_{бпом}(m)$ – ймовірності виникнення довжин m безпомилкових інтервалів між сусідніми суцільними пакетами помилок згідно моделі Бенета-Фройліха має геометричний вигляд:

$$P_{бпом}(m) = P_п(1-P_п)^{m-1}. \qquad (1)$$

Якщо розподіл P(l) також можна представити у вигляді геометричного закону

$$P(\ell) = (1-g)g^{\ell-1}, \qquad (2)$$

то середня довжина пакету помилок $\ell_{сер}$, середня довжина безпомилкового інтервалу $m_{сер}$, ймовірність помилки на біт $P_{пом}$ і ймовірність пакету помилок $P_п$ зв'язані співвідношеннями

$$\begin{aligned} m_{сер}P_п &= 1; \\ P_{пом} &= P_п\ell_{сер}; \\ \ell_{сер}(1-g) &= 1. \end{aligned} \qquad (3)$$

Для задання розглянутої моделі досить задати тільки два параметри, наприклад $P_{пом}$ і $\ell_{сер}$.

Розглянемо подію, що полягає в помилці декодування лінійного (n, к, d) блокового коду при використанні його в каналах з помилками, що групуються. Якщо на блоці з n символів код виправляє всі помилки ваги t і менші і не виправляє інших помилок, а помилки, що відбулися, відповідно до розглянутої моделі групуються в пакети з ℓ символів, то помилка декодування спостерігатиметься у разі виникнення ξ пакетів, так, що $\xi\ell > t$.

Розглянемо спрощену модель Бенета-Фройліха з непересічними пакетами помилок і можливим їх примиканням одна до одної. В цьому випадку на довжині блоку з *n* символів може відбутися не більш

$$\lambda' = \lfloor n / \ell \rfloor \qquad (4)$$

блоків помилок довжини *l*.

Число поєднань ξ пакетів на довжині з n символів визначається значенням біноміального коефіцієнту

$$C^{\xi}_{\lambda'+n-\xi l-\lambda'+\xi} = C^{\xi}_{n-\xi l+\xi}. \qquad (5)$$

Тоді ймовірність виникнення ξ пакетів довжини l помилок на блоці з n символів має такий вигляд:

$$P_{\xi}(\ell, n) = C^{\xi}_{n-\xi\ell+\xi} \cdot P_{п}(\ell)^{\xi} \cdot \left(1 - P_{п}\right)^{n-\xi\ell}. \qquad (6)$$

Остаточний вираз для оцінки ймовірності помилки декодування набере вигляду [7]:

$$P_{помд} = 1 - (1 - P_{п})^{n} - \sum_{l=1}^{n} \sum_{\xi=l,\ l<\xi\ell\le t}^{\lambda'} C^{\xi}_{n-\xi\ell+\xi} \cdot P_{п}(\ell)^{\xi} \cdot \left(1 - P_{п}\right)^{n-\xi\ell}. \qquad (7)$$

Модель з примикаючими пакетами помилок у разі фіксованого $\ell = 1$ зводиться до моделі з незалежними помилками. Дійсно, припустимо $\ell_{сер} = 1$, g = 0, $P(\ell) = 1$, $P(\ell > 1) = 0$, $P_{п} = P_{пом} = P_{п}(\ell)$ – виникають тільки одиночні помилки, які можуть примикати одна до одної. Тоді вираз (6) перепишеться у вигляді

$$P_{\xi}(\ell, n) = C^{\xi}_{n} \cdot P_{пом}{}^{\xi} \cdot \left(1 - P_{пом}\right)^{n-\xi},$$

а ймовірність помилки декодування перетвориться до

$$P_{помд} = 1 - (1 - P_{пом})^{n} - \sum_{\xi=1}^{t} C^{\xi}_{n} \cdot P_{пом}{}^{\xi} \cdot \left(1 - P_{пом}\right)^{n-\xi} =$$

$$= 1 - \sum_{\xi=0}^{t} C^{\xi}_{n} \cdot P_{пом}{}^{\xi} \cdot \left(1 - P_{пом}\right)^{n-\xi},$$

що при *i* = ξ *повністю відповідає виразу*

$$P_{помд}(n) = P\{\ell > t, n\} = \sum_{i=t+1}^{n} C^{i}_{n} P^{i}_{пом} \left(1 - P_{пом}\right)^{n-i}$$

для моделі з незалежними помилками.

На рис. 1 наведені залежності ймовірності помилкового прийому символу від співвідношення енергії сигналу до спектральної щільності потужності шуму з використанням двійкових ФМ сигналів: 1 – застосування алгебраїчного загортального коду (255, 131) в потоковій теоретико-кодовій схемі з $\rho = 0$; 2 – застосування алгебраїчного загортального коду (255, 131) в потоковій теоретико-кодовій схемі з $\rho = 0{,}2$; 3 – застосування алгебраїчного загортального коду (255, 131) в потоковій теоретико-кодовій схемі з $\rho = 0{,}4$; 4 – застосування алгебраїчного загортального коду (255, 131) в потоковій теоретико-кодовій схемі з $\rho = 0{,}6$; 5 – застосування алгебраїчного загортального коду (255, 131) в потоковій теоретико-кодовій схемі з $\rho = 0{,}8$; 6 – без кодування.

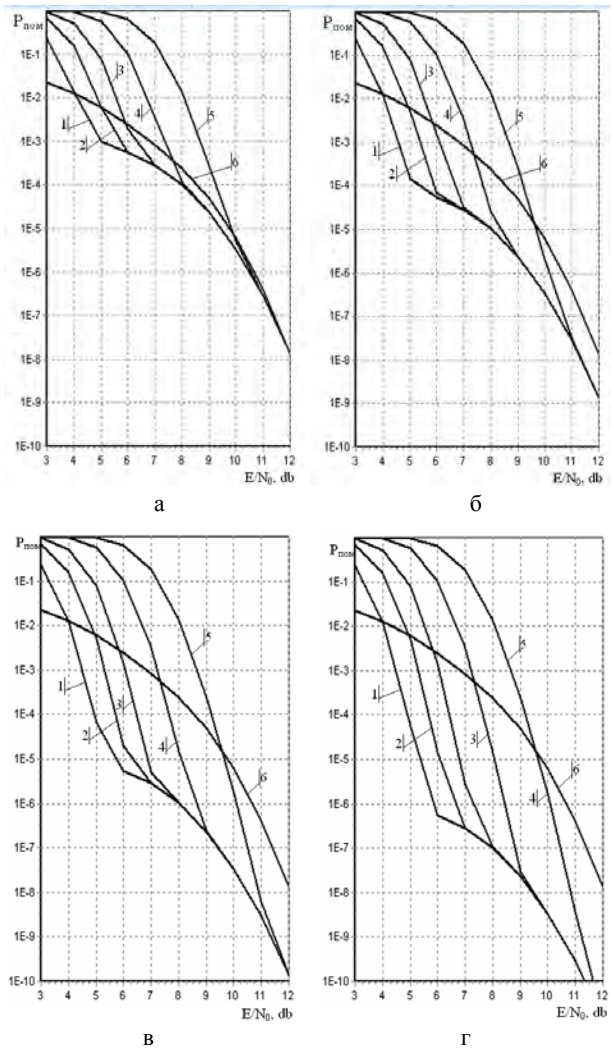

Рис. 1. Залежність ймовірності помилкового прийому символу в теоретико-кодовій схемі з алгебраїчними згортальними кодами n = 255

Розглянуті випадки для спрощеної моделі Бенета-Фройліха з непересічними пакетами помилок і можливим їх примиканням одна до одної і Рпом = 10^{-3}: а – $\ell\ \ell_{сер} = 1{,}0001$; б – $\ell_{сер} = 1{,}00001$; в – $\ell_{сер} = 1{,}000001$; г – $\ell_{сер} = 1{,}0000001$.

На рис. 2 наведені аналогічні залежності для ймовірності помилкового прийому символу з використанням двійкових ФМ сигналів і алгебраїчних згортальних (1023, 513) кодів в потоковій теоретико-кодовій схемі. Розглянуті випадки для спрощеної моделі Бенета-Фройліха з непересічними пакетами помилок і можливим їх примиканням одна до одної і Рпом = 10^{-3}: а – $\ell_{сер} = 1{,}00001$; б – $\ell_{сер} = 1{,}000001$; в – $\ell_{сер} = 1{,}0000001$; г – $\ell_{сер} = 1{,}00000001$.

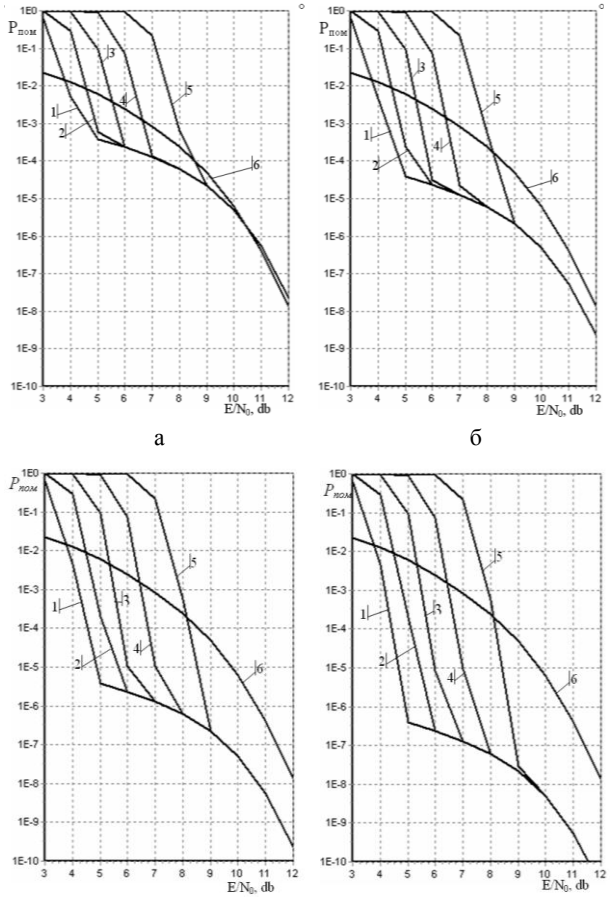

Рис. 2. Залежність ймовірності помилкового прийому символу в теоретико-кодовій схемі з алгебраїчними згортальними кодами n = 1023

Висновки

Аналіз отриманих залежностей, показує, що застосування алгебраїчних згортальних кодів в потоковій теоретико-кодовій схемі дозволяє зменшити ймовірність помилкового прийому символів в порівнянні з некодованою передачею і, таким чином, підвищити вірогідність передачі даних по каналах із слабким групуванням помилок. Із збільшенням показника групування помилок (із зростанням середньої довжини суцільного пакету помилок) виграш зменшується, а при сильному групуванні помилок стає негативною величиною, тобто застосування кодування в таких каналах приводить до енергетичного програшу. Із збільшенням, ρ як і для каналів з незалежними помилками, виграш по ймовірності помилкового прийому також зменшується, що пояснюється витратами на підвищення інформаційної таємності передачі даних

Список літератури

1. Берлекэмп Э.Р. Алгебраическая теория кодирования: Пер. с англ. / Э.Р. Берлекэмп. – М.: Мир, 1971. – 477 с.

2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2003. – 1104 с.

3. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. / Р. Блейхут – М.: Мир, 1986. – 576 с.

4. Захист інформації в комп'ютерних системах від несанкціонованого доступу / За ред. С.Г. Лаптєва. – К., 2001. – 321 с.

5. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. / Под ред. Б.С. Цыбакова. – М.: Радио и связь, 1987. – 392 с.

6. Типикин А.П. Коррекция ошибок в оптических накопителях информации // А.П. Типикин, В.В. Петров, А.Г. Бабанін. – К.: Наук. думка, 1990. – 172 с.

7. Лидл Р., Нидеррайтер Г. Конечные поля: Пер. с англ.: В 2 т. – М.: Мир, 1988. – Т. 1. – 430 с.

8. Мамаев Е. Технологии защиты информации в Интернете / Е. Мамаев. – СПб.: ИД Питер, 2001. – 848 с.

9. Саломаа А. Криптография с открытым ключом: Пер. с англ. / А. Саломаа. – М.:Мир, 1995. – 318с.

Надійшла до редколегії 26.08.2008

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ИССЛЕДОВАНИЕ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ПОТОЧНЫХ ТЕОРЕТИКО-КОДОВЫХ СХЕМ

М.И. Науменко, И.Е. Кужель

Проведен расчет показателей достоверности передачи информации в каналах с ошибками, которые группируются на основе использования математической модели Бенета-фройлиха. Дана оценка энергетического выигрыша от применения предложенных теоретико-кодовых схем в каналах передачи данные с независимыми ошибками и ошибками, которые группируются. Рассмотрены зависимости вероятности ошибочного приема символа в теоретико-кодовой схеме из сверточных кодов алгебраизма. Проведен анализ применения сверточных кодов алгебраизма в поточной теоретико-кодовой схеме.

Ключевые слова: *помехоустойчивая кодировка, теоретико-кодовые схемы, пакет ошибок, вероятность, модель.*

RESEARCH OF AUTHENTICITY OF TRANSMISSION INFORMATION AT THE USE OF ПОТОЧНЫХ CODED-THEORETICAL CHARTS

M.I. Naumenko, I.E.Kuzhel'

The calculation of indexes of authenticity of passing to information is conducted in ductings with errors which form a group on the basis of the use of mathematical model of Beneta-froylikha. The estimation of the power winning is given from application of the offered coded-theoretical charts in ductings of transmission information with independent errors and errors which form a group. Dependences of probability of erroneous reception of character are considered in a coded-theoretical chart from the convolutional kodas of algebra. The analysis of application of convolutional kodas of algebra is conducted in a поточной coded-theoretical chart.

Keywords: *antijamming code, coded-theoretical charts, burst of errors, probability, model.*