УДК 621.396.96
Ю. М. БОЙКО, доктор техн. наук, доцент;
Д. А. МАКАРИШКІН, канд. техн. наук, доцент;
О. І. ПАСІЧНИК, магістрант,
Хмельницький національний університет

Дослідження ефективності алгоритмів канального кодування в захищених телекомунікаційних системах передавання інформації

Розглянуто механізми підвищення захищеності телекомунікаційних систем завдяки застосуванню алгоритмів завадостійкого канального кодування. Сформовано структуру каналу передавання інформації з турбокодуванням. Розглянуто блок-діаграму кодера турбокоду для формування схеми захищеної телекомунікаційної системи.

Формалізовано принципи декодування турбокоду використанням ітеративного декодера. Описано принципи та реалізацію процесу синхронізації для турбокодів на основі використання прикріпленого маркера синхронізації.

Наведено експериментальні дані для визначення енергетичного виграшу кодування при різних довжинах блоків турбокодів.

Запропоновано та досліджено схеми реалізації кодера з перемежуванням бітів даних для складових кодів при реалізації телекомунікаційної системи з канальним кодуванням.

Описано фреймову структуру пакета даних для передавання інформації кодом Ріда–Соломона. Розроблено імітаційну схему для дослідження принципів формування сигналів на основі каскадних кодів у телекомунікаційних системах.

Наведено результати дослідження імітаційної схеми каналу передавання інформації в телекомунікаційних системах із каскадним кодуванням при визначенні енергетичного виграшу та усунення ефекту насичення турбокодів.

Ключові слова: канальне кодування; фазова маніпуляція; сигнально-кодова конструкція; телекомунікаційна система.

Вступ. Постановка проблеми

Захищеність телекомунікаційних систем — важлива їх властивість. Загалом захищеною телекомунікаційною системою можна вважати таку систему, яка виконує поставлені завдання за наявності завадових впливів як природного походження, так і спрямованої дії. Зрештою завадові впливи будемо розглядати як адитивні шуми та мультиплікативні завади. Наявність таких впливів висуває перед захищеною телекомунікаційною системою вимоги щодо оптимізації характеристик завадостійкості завдяки застосуванню алгоритмів завадостійкого канального кодування [1–7].

Канальне кодування — це метод кодування, за допомогою якого дані можуть бути відправлені з джерела до пункту призначення таким чином, щоб окремі повідомлення легко було відрізнити одне від одного. Це дозволяє відновити дані з низькою ймовірністю помилки. При цьому канальний кодер являє собою той пристрій, який приймає потік двійкових даних від первинного джерела і виробляє вихідний сигнал [1; 7; 8]. Якщо правильно вибрати код для конкретного телекомунікаційного каналу, то правильно сконструйований декодер зможе відновити вихідні двійкові дані навіть тоді, коли форму сигналу було спотворено шумами та завадами в каналі. Слід також зазначити, що за наявності вірогідної інформації стосовно характеристик телекомунікаційного каналу канальне кодування згідно з вибраною схемою забезпечить вищу загальну пропускну здатність каналу, ніж у разі некодованих даних, причому з меншими витратами енергії. Йтиметься про підвищення енергетичного виграшу. Окрім того, канальне кодування дозволяє знизити загальну частоту появи помилкових бітів порівняно з некодованими системами при використанні тієї самої енергії для передавання даних у розрахунку на біт інформації.

Акцентуємо увагу на такому аспекті: для підвищення ефективності декодування інформації вибрані для канального кодування коди мають бути якомога довші [2], бо наявність шумів і завад вимагає їх усереднення для великої кількості символів. Загалом можна виокремити такі проблемні аспекти канального кодування в захищених телекомунікаційних системах. Має бути здійснено пошук кодів, які повинні забезпечити вимоги щодо виправлення помилок; пошук та розробку практично реалізованого методу кодування/декодування; пошук методу прийняття рішення на приймальному боці, тобто методу виправлення помилок.

Пошук розв'язання суперечності через поєднання несумісних, здавалося б, властивостей «щільних» багатопозиційних сигналів (висока частотна ефективність) і завадостійких кодів (висока енергетична ефективність) в єдиній конструкції, що забезпечує одночасне зростання як енергетичної, так і частотної ефективності, спонукає до постановки ***актуальної проблеми*** — підвищення ефективності обробки сигналів у захищених телекомунікаційних системах з обмеженою смугою пропускання та потужністю сигналів при передаванні інформації за наявності завад. Розв'язання такої проблеми можливе шляхом побудови кодів, для яких можна математично довести їх спроможність задовільно виправляти помилки. Вочевидь, такі коди повинні мати особливу математичну структуру, яка надалі може бути використана для задоволення вимог щодо практичної реалізації алгоритмів кодування і декодування, та бути «прозорими» щодо неоднозначності фази сигналів при формуванні сигнально-кодової конструкції (СКК). Поєднання ефективного кодування в захищених телекомунікаційних каналах із низьким рівнем помилок і складних алгоритмів адаптивного стиснення даних може привести до істотного підвищення загальної продуктивності телекомунікаційних систем.

Мета і завдання дослідження

Розвиток описаних у [1–10] засобів підвищення завадостійкості у пропонованій статті проведено дослідження завадостійкості телекомунікаційних систем із каскадним кодуванням, зокрема з використанням схем каскадного кодування на основі турбокодів (ТК) [1; 2; 6]. Здійснено пошук ансамблів багатопозиційних сигналів при завадостійкому кодуванні в захищених телекомунікаційних системах для реалізації СКК, області яких у багатопозиційному просторі компактні (для забезпечення частотної ефективності) і достатньо далеко розсіяні (щоб забезпечити високу енергетичну ефективність).

Тому метою дослідження, викладеного в статті, є розв'язання завдання, яке полягає в підвищенні ефективності формування та оброблення сигналів у телекомунікаційних системах, що, у свою чергу, дасть змогу вдосконалити апаратну та алгоритмічну частини пристроїв обробки сигналів з урахуванням вибору параметрів останніх для забезпечення максимальної пропускної здатності захищених телекомунікаційних систем, установлення оптимальної СКК, за якої реалізується необхідна завадостійкість у разі використання цифрової модуляції.

Аналіз останніх досліджень і публікацій із даної тематики та синтез структури канального кодування

Основну увагу зосередимо на можливостях підвищення енергетичного виграшу кодування (ЕВК) у разі формування схеми телекомунікаційної системи. Зокрема, в [1; 2] показано, що й досі найбільш помітним досягненням теорії завадостійкого кодування є розробка ТК. Для систем із турбокодуванням декодування полягає в тому, щоб передати м'яку схему прийняття рішення з виходу одного декодера на вхід іншого і повторювати цю процедуру доти, доки не буде отримано надійне рішення [2]. Ці коди можуть майже досягати межі Шеннона при достатній складності декодування. Турбокоди перевершують навіть найпотужніші з відомих кодів, але, що ще важливіше, вони набагато простіші для декодування. Було виявлено [1–6], що ефективні ТК можуть забезпечувати відстань близько 0,8 дБ від теоретичної межі при ймовірності бітової помилки (BER) на рівні 10^{-6}. Застосовуючи такі коди, важливо мати на увазі, що гранична продуктивність їх використання в телекомунікаційних каналах залежить від швидкості кодування [7]. В [1–10] докладно описано процес канального кодування в разі використання ТК і подано алгоритм декодування таких кодів на основі критерію максимальної апостеріорної ймовірності (МАЙ). Тому спинимось на інших можливих підходах до формування і декодування таких кодів.

Загалом основне питання, яке буде розглянуто далі, стосується можливості поєднання ТК і лінійних циклічних кодів на основі кодів Боуза–Чоудхурі–Хоквингема (БЧХ) для підвищення ефективності використання СКК із фазовою багатопозиційною модуляцією в телекомунікаційних і телеметричних каналах передавання даних.

Турбокод являє собою комбінацію двох простих рекурсивних згорткових кодів, кожний з яких використовує невелику кількість станів. Ці прості згорткові коди утворюють блокову структуру. Для блока з l-інформаційних бітів кожний компонент коду генерує набір бітів парності. Таким чином, ТК складається з інформаційних бітів і наборів бітів парності.

Реалізацію схеми телекомунікаційного каналу на основі турбокодів унаочнює рис. 1.

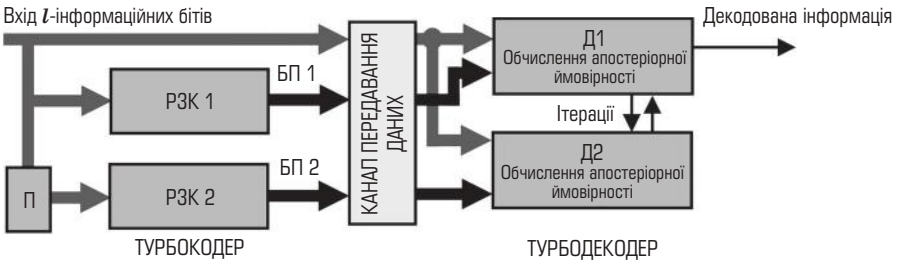


Рис. 1. Структурна схема телекомунікаційного каналу на основі турбокодів:
П — перемежувач; РЗК — рекурсивний згортковий кодер; Д — декодер; БП — біти парності (перевірні біти)

Вхідні дані потрапляють на другий РЗК через перемежувач. Завдання підвищення ефективності полягає в правильному виборі типу перемежувача. Інформаційні блоки, які відповідають підтвердженим помилкам кодових слів у першому коді, будуть відповідати усталеним помилкам у кодових словах другого коду. Для турбодекодування візьмемо два прості декодери. Кожний декодер надсилає оцінки правдоподібності декодованих бітів на інший декодер і використовує відповідні оцінки від нього як апріорну ймовірність. Складові декодери реалізують алгоритм побітового декодування, який вимагає такої самої кількості станів, як добре відомий алгоритм Вітербі [6; 7]. Для досягнення задовільної збіжності при декодуванні застосуємо ітераційну процедуру між виходами двох декодерів. У кінцевому результаті дістанемо «жорстку» оцінку правдоподібності. Для досягнення максимальної продуктивності задіємо ТК із великою довжиною блоків і відповідні великі перемежувачі. Загалом розмір перемежувача відчутно впливає на вимоги до буфера обміну і затримки декодування, але майже не впливає на швидкість декодування і складність декодера. Розгорнуті структурні схеми кодера та декодера наведено на рис. 2 і 3.

Зокрема, на рис. 2 подано блок-діаграму турбокодера, що містить два згорткові рекурсивні кодери довжиною $l = 5$, які реалізовано на регістрах зсуву зі зворотними зв'язками. Така конструкція має особливість порівняно з класичною для згорткових кодів [7]: кожний кодовий блок турбокоду запускається додатково для $(l - 1)$-го біта наприкінці кадру інформаційної послідовності. Після кодування останнього біта в кадрі крайній лівий суматор у кожному компонентному кодері приймає дві копії одного й того самого біта зворотного зв'язку та переводить у нульовий стан їх виходи. Після $(l - 1)$-го біта чотири комірки пам'яті заповнюються нулями, але

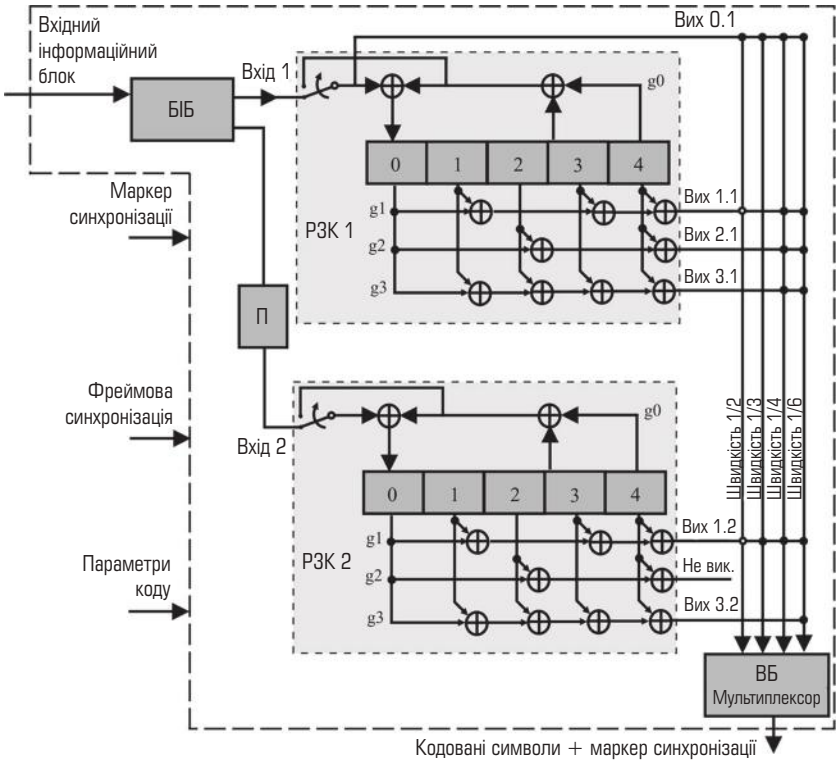


Рис. 2. Блок-діаграма кодера турбокоду:
П — перемежувач; РЗК — рекурсивний згортковий кодер; Д — декодер;
БІБ — вхідний буфер інформаційного блока; ВБ — вихідний буфер

в інші моменти часу кодер продовжує видавати ненульові кодовані символи. У поданій конструкції кодера швидкості кодування становили 1/3, 1/4 і 1/6 без процедури виколювання. Виколювання використовували при швидкості кодування 1/2. Для довжин кадрів 1784 до 16384 біт брали різні перемежувачі, зокрема псевдовипадковий і регулярний, які працюють за правилом перестановлень із записами результатів у довідкові таблиці. У схемі, наведений на рис. 2, передбачено елементи синхронізації. Зокрема, маркер синхронізації слугує для контролю стану вхідного буфера (контроль вмісту буфера); стосовно вихідного буфера (мультиплексора) він фіксує покажчик кадрової синхронізації; у компонентних кодерах фіксує момент закінчення кодового блока. Слід зауважити, що процес кодування неодмінно супроводжується часовими затримками сигналу (таймінгами) [7], причому весь інформаційний блок із l-бітів повинен бути прочитаний до подачі наступного блока на кодування.

Далі запропоновано конструкцію каскадного коду на основі компонентного ТК та коду Ріда–Соломона (РС). Тому при синтезі структури кодера ТК розставимо такі акценти.

Реалізація турбокодера має свої особливості. Зокрема, інформаційний блок повинен буферизуватись та зчитуватись у певному порядку в процесі кодування. Така буферизація відсутня в згортковому кодері, а розмір буфера порівнянний із розміром перемежувача для коду РС. Таким чином, турбокодер загалом замінює каскадну конструкцію на основі згорткового коду та коду РС і не є альтернативою згорткового кодера в згаданій каскадній конструкції. Проте для підвищення ефективності каскадних конструкцій далі буде запропоновано поєднання таких кодів.

Розглянемо процес декодування ТК. У турбодекодері використовується ітеративний алгоритм декодування. Кожний компонентний декодер дає оцінку правдоподібності, причому прийняті некодовані інформаційні символи доступні обом декодерам для здійснення цих оцінок. Кожний декодер відправляє свої оцінки правдоподібності на інший декодер і використовує відповідні оцінки від іншого декодера для визначення нових оцінок правдоподібності шляхом вилучення зайвої інформації, яка міститься в оцінках іншого декодера, на основі символів парності, доступних тільки для нього. Загалом можна використати такі алгоритми декодування в декодері турбокоду: максимуму апостеріорної ймовірності (МАЙ), логарифмічний МАЙ (його модифікацію max-log-MAP, APP), алгоритм «м'якого» декодування за Вітербі [7]. У результатах моделювання, проведеного далі, здійснено порівняння різних алгоритмів. За базовий узято алгоритм побітового декодування при визначенні МАЙ, тим більш що, як показали дослідження, його складність можна порівняти зі складністю алгоритму Вітербі. Нагадаємо вказівку щодо ітераційного процесу між виходами двох складових декодерів (див. рис. 1), здійснюваного для досягнення задовільної збіжності.

Схема декодера, подана на рис. 3, містить два детектори МАЙ, що їх позначено як ДМВМВ (SISO) — декодер із «м'яким» входом та «м'яким» виходом; перемежувач і деперемежувач, використовувані для поновлення вихідного порядку символів; прийняті після демодулятора інформаційні біти та параметри коду (перевірні біти) $G_{\text{к}}y_j$, а також апріорну інформацію (інформацію для оцінювання значення інформаційних бітів даних) $G(u_j)$ із відповідних декодерів ДМВМВ. Схема такого складового декодера ітеративно оновлює апріорну інформацію протягом фіксованого числа ітерацій декодування і потім виводить біти рішення.

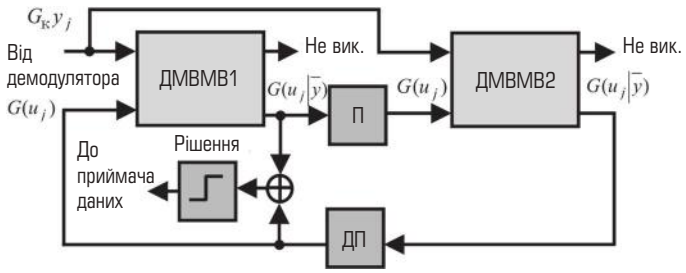


Рис. 3. Блок-схема ітеративного турбодекодера:
ДМВМВ (SISO) — декодер із «м'яким» входом та «м'яким» виходом; П — перемежувач; ДП — деперемежувач

Подамо вихідні рішення як «м'які» відносно декодованих бітів даних. Використаємо логарифм відношення функцій правдоподібності, причому знак цього відношення визначає значення декодованого біта даних: додатне — 1; від'ємне — 0; модуль — надійне рішення [1]. Запишемо логарифмічне відношення функцій правдоподібності для кожного інформаційного символа u_l в такий спосіб:

$$G(u_l) = \ln\left[\frac{p(u_l = +1)}{p(u_l = -1)}\right], \quad (1)$$

де $p(u_l = n)$ — імовірність події $u_l = n$ при $n = \pm 1$.

Декодер ДМВМВ1 на основі інформації, прийнятої з каналу передавання даних, формує оцінку інформаційних бітів даних. Далі з отриманої оцінки $G\left(u_k \middle| \bar{y}\right)$ шляхом виключення апріорної інформації та отриманих із каналу систематичних символів утворюється зовнішня інформація. Цей процес подамо в такому формалізованому вигляді:

$$G_з(u_l) = G\left(u_l \middle| \bar{y}\right) - G_a y_{ls} - G(u_l), \quad (2)$$

де для дискретного гауссівського каналу без пам'яті (AWGN) член $G_a = 2/\sigma^2$ визначає надійність каналу, а σ^2 — дисперсію шуму.

Другий ДМВМВ2 використовує отриману інформацію (апріорну) для проведення власного оцінювання.

Описані процеси належать першій ітерації. На другій ітерації процес декодування виконується з урахуванням апріорної оцінки другого декодера ДМВМВ2. Так само виконується кілька ітерацій, найчастіше 10 [2].

Імовірність бітової помилки для ТК набирає вигляду [1; 5]:

$$P_{пом} \le \sum_{i=d}^{N} \frac{c_i}{l} p_i, \quad (3)$$

де N — довжина кодового блока; l — розмір блока, який піддається перемежуванню; c_i — загальна інформаційна вага всіх кодових слів вагою i; p_i — імовірність вибору неправильного кодового слова, яке відрізняється від правильного в i позиціях.

При цьому p_i визначаємо аналітично за допомогою таких міркувань. Оцінювання ймовірності $P_{пом}$ бітової та $P_ф$ фреймової помилки лінійного блокового коду довжиною l при декодуванні за допомогою декодера максимальної правдоподібності можна здійснити, скориставшись такими співвідношеннями:

$$P_ф \le \sum_{j=1}^{L} n_j p_i(j), \quad (4)$$

$$P_{пом} \le \sum_{j=1}^{L} \frac{j}{m} n_j p_i(j), \quad (5)$$

де m — кількість інформаційних символів коду; n_j — кількість кодових слів вагою j;

$$p_i(j) = \begin{cases} \sum\limits_{i=(j+1)/2}^{j} C_j^i (1 - p_{вх})^{j-1}; \\ 0{,}5 C_j^{j/2} p_{вх}^{j/2} (1-p)^{j/2} + \sum\limits_{i=(j/2)+1}^{j} C_j^i p_{вх}^i (1 - p_{вх})^{j-1}. \end{cases} \quad (6)$$

Тут перше рівняння справджується для дискретного симетричного каналу при непарних j, а друге — при парних j.

У разі AWGN каналу маємо:

$$p_i(j) = \Phi\left(\sqrt{2jE_c/N_0}\right), \quad (7)$$

де $\Phi(x)$ — інтеграл імовірності, $\Phi(x) = 1/\sqrt{2\pi} \int\limits_{-\infty}^{x} e^{\frac{t^2}{2}} dt$; $p_{вх}$ — імовірність бітової помилки в каналі передавання даних; E_c/N_0 — відношення сигнал/шум у каналі.

Спинимося на питанні синхронізації при турбокодуванні. Синхронізація турбокодованих блоків досягається за рахунок використання маркера синхронізації (рис. 4). При цьому довжина блока ТК і маркера синхронізації обернено пропорційні до номінальної швидкості R кодування.

Отже, ефективність синхронізації залежить від швидкості кодування. На приймальному боці телекомунікаційного каналу маркер синхронізації ідентифікується за певними ознаками своєї структури.

Варто зазначити, що кожний із декодерів складового декодера (див. рис. 3) не завжди може правильно виявити ефективний розмір маркера синхронізації, а це дуже важливо. Адже в разі декодування довгого ТК декодери складового декодера повинні чітко ідентифікувати межі кодового блока, у тому числі з урахуванням перемежених і деперемежених даних у структурі декодера. Тому зазвичай до складу маркера синхронізації включається канальний символ (домен), який визначає метод кадрової синхронізації.

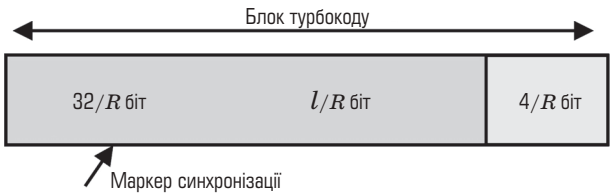


Рис. 4. Схема результуючого блока турбокоду (див. рис. 2) із прикріпленим маркером синхронізації: l — довжина блока інформаційних даних; R — заявна швидкість кодування

Результати визначення завадостійкості телекомунікаційного каналу передавання даних на основі ТК різної довжини ілюструє рис. 5 [2].

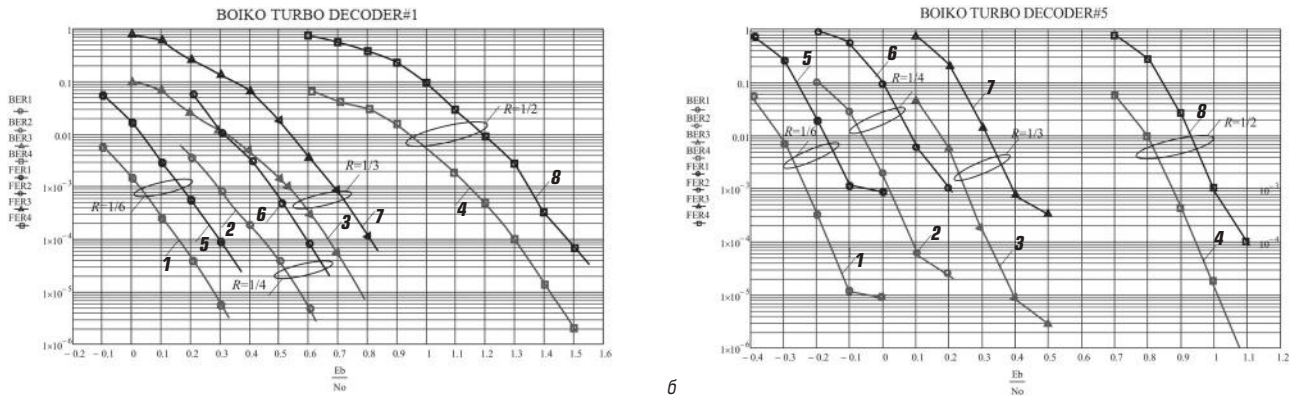


Рис. 5. Графіки залежності для визначення BER і FER при швидкості кодування: R = 1/2; 1/4; 1/3 і 1/6 для турбокодів із розміром блока: 1784 бітів (*а*); 16384 бітів (*б*) (10 ітерацій): *1* — BER (R = 1/6); *2* — BER (R = 1/4); *3* — BER (R = 1/3); *4* — BER (R = 1/2); *5* — FER (R = 1/6); *6* — FER (R = 1/4); *7* — FER (R = 1/3); *8* — FER (R = 1/2)

Дані про помилки, виражені через імовірність BER бітових помилок, що визначає частоту помилок для окремих бітів, та ймовірність FER помилок кадрів (фреймів), наведено в табл. 1 і 2.

Таблиця 1

Експериментальні дані щодо енергетичного виграшу кодування для турбокоду з розміром блока 1784 бітів

Швидкість кодування	Рівень BER	Рівень FER	ЕВК (енергетичний виграш кодування), дБ	
			BER	FER
1/2	10^{-4}	10^{-4}	1,1	0,83
1/3	10^{-4}	10^{-4}	1,65	1,5
1/4	10^{-4}	10^{-4}	1,85	1,7
1/6	10^{-4}	10^{-4}	2,15	2,0

Таблиця 2

Експериментальні дані щодо енергетичного виграшу кодування для турбокоду з розміром блока 16384 бітів

Швидкість кодування	Рівень BER	Рівень FER	ЕВК (енергетичний виграш кодування), дБ	
			BER	FER
1/2	10^{-4}	10^{-4}	1,35	1,20
1/3	10^{-4}	10^{-4}	1,98	Насичення турбокоду
1/4	10^{-4}	10^{-4}	2,21	Насичення турбокоду
1/6	10^{-4}	10^{-4}	2,46	Насичення турбокоду

Відомості [2], наведені на рис. 4 і в табл. 1, дозволяють дійти такого висновку: збільшення розміру блока ТК призводить зрештою до його насичення, причому крутість характеристики ТК стає менш вираженою зі зростанням відношення E_b/N_0 (E_b — енергія, необхідна для передавання одного біта інформації; N_0 — спектральна густина потужності шуму). Досягти малої ймовірності помилок, наприклад 10^{-12}, за допомогою ТК можна лише при великих значеннях відношення сигнал/шум (E_b/N_0).

Розглянемо питання вибору перемежувача в схемі канального турбокодування, проаналізувавши наведені на рис. 6 залежності вихідних позицій (Output) бітів у кодованих блоках від вхідних (Input) для різних типів перемежувачів.

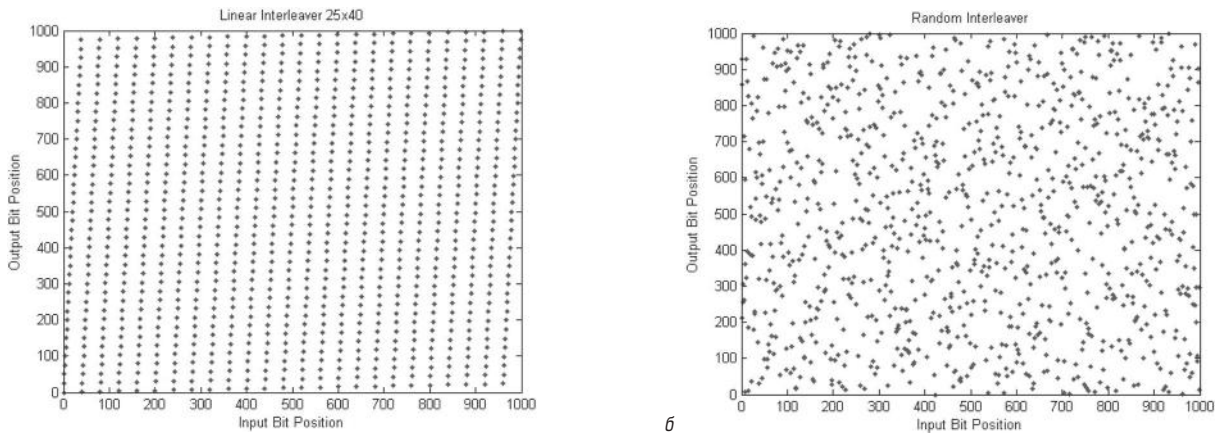


Рис. 6. Залежність вихідної позиції бітів у блоці від вхідної їх позиції для різних типів перемежувачів: *а* — періодичний перемежувач; *б* — псевдовипадковий перемежувач

Загалом кажучи, можна реалізувати як періодичні, так і псевдовипадкові схеми перемежування даних. Періодичні перемежувачі поділяються на блокові та згорткові. Перевага згорткових перемежувачів полягає в тому, що затримка і ємність пам'яті в цьому разі вдвічі менша, ніж при застосуванні блокових пристроїв перемежування. Для турбокодування вибір перемежувача досить важливий, оскільки його структура безпосередньо впливає на мінімальну відстань та кількість кодових слів низької ваги, а ті, у свою чергу, згідно з формулами (1) – (7), безпосередньо впливають на ефективність ТК. У разі псевдовипадкового перемежувача біти початкового блока в перемеженому блоці розташовуються псевдовипадково, і це, зрештою, досить позитивно впливає на загальну ефективність ТК.

З'ясуємо тепер, як кількість ітерацій, згаданих в опису поданої на рис. 1 схеми, впливає на ефективність декодування та завадостійкість. Візьмемо ТК $(7, 5)_8$ при $R = 1/2$ із виколюванням (перфорований код), довжина кадру для перемежування $l = 400$ бітів. Декодування було проведено за алгоритмом log-МАЙ. Залежність імовірності помилки від E_b/N_0, отриману при моделюванні, подано на рис. 7, де по осях відкладено відповідно BER, відношення E_b/N_0, дБ, та кількість ітерацій при декодуванні. Результат моделювання являє собою поверхню, утворену перерізами, кожний з яких визначає залежність імовірності бітової помилки від E_b/N_0 при фіксованій кількості ітерацій. Аналіз графіка показує, що характеристики коду та завадостійкість поліпшуються зі збільшенням кількості ітерацій, але вже після сьомої ітерації таке поліпшення досить незначне. Оцінимо енергетичний виграш кодування (ЕВК) досліджуваного ТК при згортковому канальному кодуванні за треліс-структурою: ЗК (poly2trellis (7, [171; 133])) та диференціальною квадратурною фазовою маніпуляцією (DQPSK) — «жорстке» рішення. Значення відношення E_b/N_0 для рівня BER $= 10^{-4}$ становить відповідно 2,3 і 8,2 дБ. Отже, ЕВК ≈ 5,9 дБ.

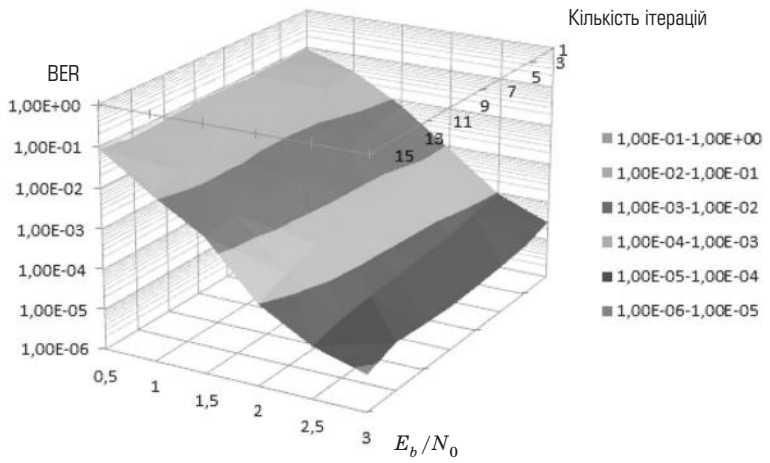
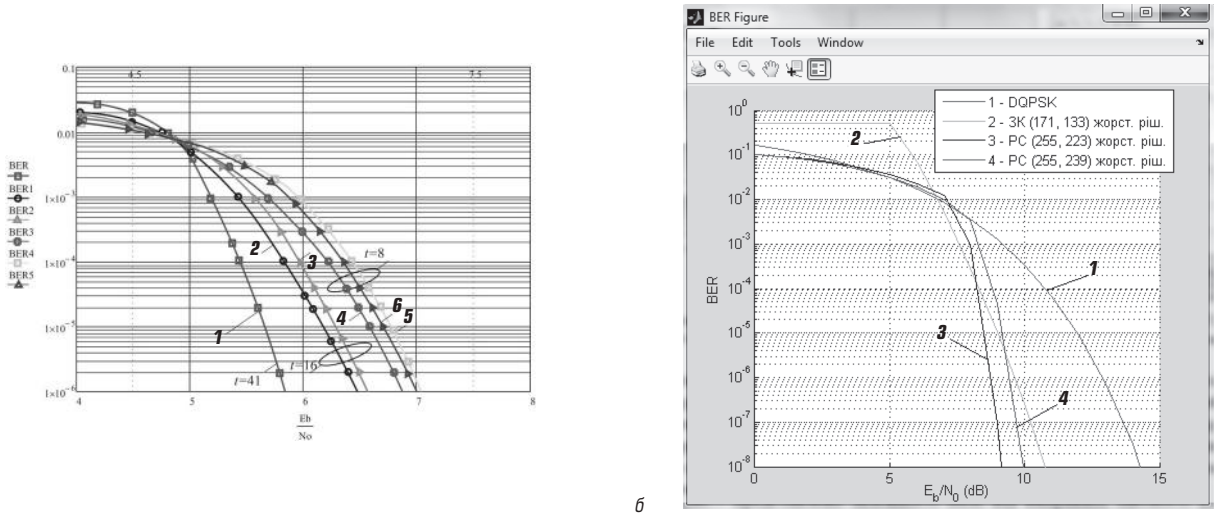


Рис. 7. Залежність завадостійкості від кількості ітерацій для турбокоду $(7,5)_8$

Формування та дослідження схеми каскадної конструкції канального кодування з використанням турбокодів

Розглянемо можливості каскадних кодів. Такі коди застосуємо для утворення коду з великою довжиною блока і високою коригуючою властивістю. Насамперед зазначимо, що декодер коду РС створює на виході неспотворену послідовність, якщо послідовність прийнятих символів відрізняється від справжнього слова не більш як на t символів [8–10]. Тоді декодер автоматично визначає кількість помилок.

Каскадний код використаємо для усунення ефекту насичення турбокодів, розглянутих раніше, а також для підвищення завадостійкості. Як зовнішній код візьмемо код РС, а як внутрішній — ТК. З метою аналізу ефективності такої каскадної конструкції подамо результати дослідження завадостійкості кодів РС і каскадних кодів зі структурою РС + ЗК + QPSK: зовнішній кодер РС, а внутрішній — згортковий (ЗК); модуляція квадратурна фазова QPSK (рис. 8).



а *б*

Рис. 8. Графіки залежності для оцінювання: *а* — завадостійкості кодів Ріда–Соломона (255, 173) — *1*; (157, 125) — *2*; (255, 223) — *3*; (97, 81) — *4*; (255, 239) — *5*; (204, 188) — *6*; *б* — енергетичного виграшу кодування

На відміну від «м'яких» рішень, характерних для згорткових кодів, вихід декодера РС є «жорстким», а отже, декодер діє на символ алфавіту, що використовується при кодуванні.

Зауважимо, що наведені на рис. 8, *а* залежності BER від виправної здатності кодів РС, дозволяють встановити, що найкращі показники має код РС (255, 173) при $t = 41$.

Результати дослідження завадостійкості для каскадних і згорткових кодів подано на рис. 9 і 10 при таких СКК: РС(255, 223) + ЗК і РС(255, 239) + ЗК. Як бачимо, ефективність використання каскадних кодів вища, ніж кодів РС, використовуваних окремо (див., наприклад, рис. 9, криві 1 і 5 — енергетичний виграш становить майже 3,2 дБ (BER = 10^{-7})).

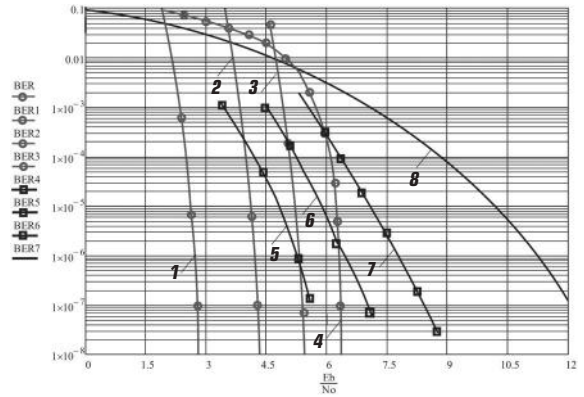


Рис. 9. Графіки залежності BER від E_b/N_0 для згорткового та каскадного кодів при різних швидкостях кодування і t = 16: *1* — РС + ЗК(255, 223) при R = 1/2; *2* — РС + ЗК(255, 223) при R = 3/4; *3* — РС + ЗК(255, 223) при R = 7/8; *4* — РС(255, 223); *5* — ЗК при R = 1/2; *6* — ЗК при R = 3/4; *7* — ЗК при R = 7/8; *8* — некодована QPSK

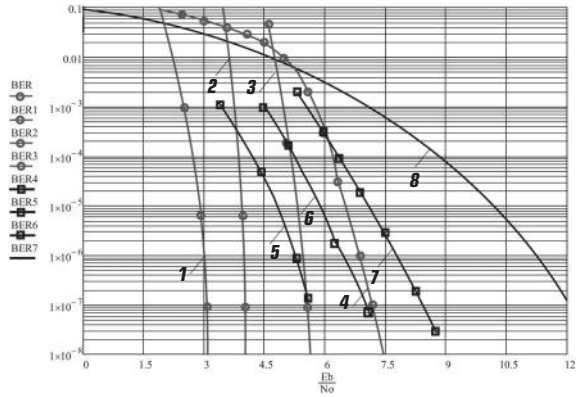


Рис. 10. Графіки залежності BER від E_b/N_0 для згорткового та каскадного кодів при різних швидкостях кодування і t = 8: *1* — РС + ЗК(255, 239) при R = 1/2; *2* — РС + ЗК(255, 239) при R = 3/4; *3* — РС + ЗК(255, 239) при R = 7/8; *4* — РС(255, 239); *5* — ЗК при R = 1/2; *6* — ЗК при R = 3/4; *7* — ЗК при R = 7/8; *8* — некодована QPSK

Спинимось на основних вимогах до кодів РС. Це недвійкові коди (підвид кодів БЧХ), що мають такі параметри: довжина блока $n = q - 1$ (зазвичай $q = 2^m$, тоді кодом виправляються 2^m-ні символи); кількість k інформаційних символів змінюється від 1 до $n - 1$; мінімальна кодова відстань $d_{\min} = n - k + 1$; кодова швидкість $R = k/n$. Для подання кодів РС використано породжувальний поліном виду

$$g(x) = (x - \alpha)(x - \alpha^2)\ldots(x - \alpha^{2t}), \qquad (8)$$

де $t = \left[\frac{1}{2}(d_{\min} - 1)\right]$; α — елемент поля Галуа GF(q^m) [1; 2].

Породжувальний поліном, як бачимо, має степінь $2t$, а отже, можна використати $2t$ перевірних символів для виправлення t помилок.

Описані далі схеми канального кодування на основі алгоритму декодування «жорстких» рішень слугуватимуть для того, аби можна було застосувати такі довгі коди при формуванні каскадної конструкції та використанні в телекомунікаційному каналі багатопозиційної фазової маніпуляції.

Для зовнішнього кодера пропонується взяти кодер РС із довжиною блока $n = 255$. Код має розмір інформаційного блока $k = 223$; мінімальна Хеммінгова відстань $d = 33$. Код може виправити 16 помилок. Блок-схему коду подано на рис. 11. Структура коду містить 223 інформаційні та 32 перевірні символи. Породжувальний многочлен будуємо в полі Галуа GF(2^8) [1; 2; 10]. Початкова інформаційна кодова комбінація являє собою многочлен $g(x) = x^8 + x^7 + x + 1$. Вибір цього многочлена зумовлено передусім необхідністю мінімізації технічної складності шифраторів.

Рис. 11. Структура коду Ріда–Соломона (255, 223)

Загальну структуру фрейма, який використаємо при канальному кодуванні, унаочнює рис. 12.

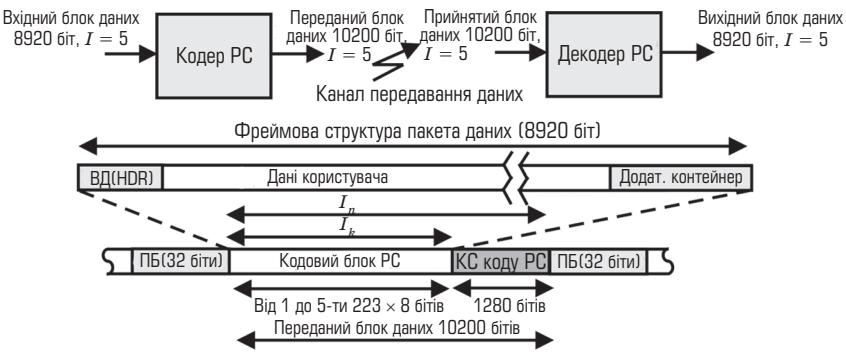


Рис. 12. Фреймова структура пакета даних для передавання інформації кодом Ріда–Соломона: ВД — заголовок вхідних фреймових даних (header); ПБ — перевірні біти; КС — контрольні біти синхронізації, I — довжина перемежувача, I = 5

Узагальнену схему кодера згідно з формою породжувального многочлена (8) зображено на рис. 13.

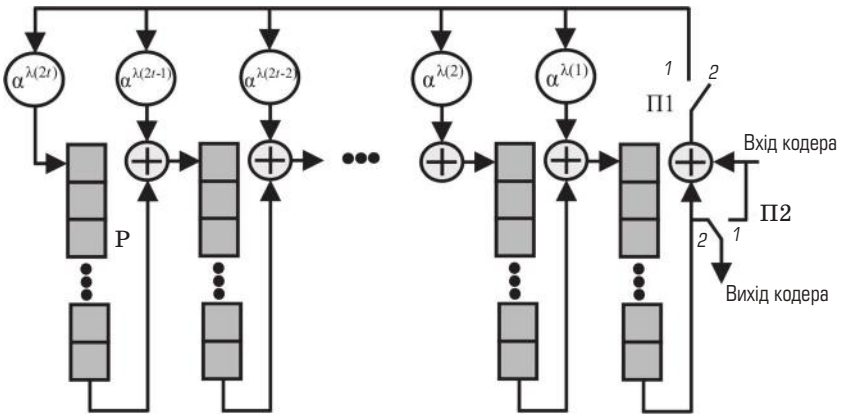


Рис. 13. Схема кодера РС із перемежуванням даних: Р — регістри зсуву; П — перемикачі; α — елемент поля Галуа

Кодер являє собою цифровий автомат, усі операції в якому виконуються в полі Галуа за модулем примітивного полінома [7]. Операції додавання виконуються за модулем два, а для виконання множення слугують таблиці логарифмів і антилогарифмів. На вхід кодера надходить інформація в байтовій формі. Інформаційні символи надходять на вихід кодера без затримки, якщо перемикачі П1 і П2 перебувають у положенні *1*. Після надходження k інформаційних символів вхід кодера відмикається, П1 і П2 переводяться в положення *2* і на вихід надходять $n - k$ перевірних символів, які містяться в регістрах зсуву (див. рис. 13).

Особливість цієї схеми кодера полягає в тому, що вона містить N регістрів. У схемі використано принцип блокового перемежування, який можна описати матрицею, яка містить X рядків і Y стовпців. Тоді при передаванні даних інформація зчитується по стовпцях, а на приймальному боці — по рядках. Параметр Y дорівнює довжині кодового слова блокового коду. Використовуючи такий принцип у схемі кодера, досягаємо такої переваги: оскільки після кодування кодом РС довжина блока кратна $X \cdot Y$, то дістаємо схему, в якій немає процесу очищення регістрів. Надлишковість такої схеми, зумовлена наявністю перемежувача, буде нульовою. У пристрої кодера Y дорівнює довжині кодового слова коду РС, і тоді загальна затримка внаслідок перемежування буде дорівнювати затримці у згортковому пристрої перемежування внутрішнього коду. Схема такого кодера обробляє циклічно вхідну інформаційну послідовність в байтовій формі.

Асимптотичну оцінку ймовірності помилки в кодовому блоці подамо так [1]:

$$p_{\text{КБ}} = \sum_{i=t+1}^{n} C_n^i \, p_0^i \left(1 - p_0\right)^{n-i}. \tag{9}$$

Тут $p_0 = \dfrac{q/2}{q-1} p_{\text{с}}$ — імовірність бітової помилки, де $p_{\text{с}}$ — імовірність помилки для q-го символа,

$$p_{\text{с}} \le \frac{1}{n} \sum_{i=t+1}^{n} (i+t) C_n^i \, p_0^i \left(1 - p_0\right)^{n-i}. \tag{10}$$

Залежності для визначення ймовірності бітових помилок (див. рис. 9 і 10) отримано методом математичного моделювання для досліджуваних кодів РС та для випадку каскадного кодування РС + ЗК.

Розглянемо наведені на рис. 14 і 15 результати моделювання BER для таких СКК, як РС(255, 223) ($t = 16$) + ЗК (7, 1/2), при зміні глибини перемежування від $I = 1$ до $I = 16$ для різних швидкостей ЗК.

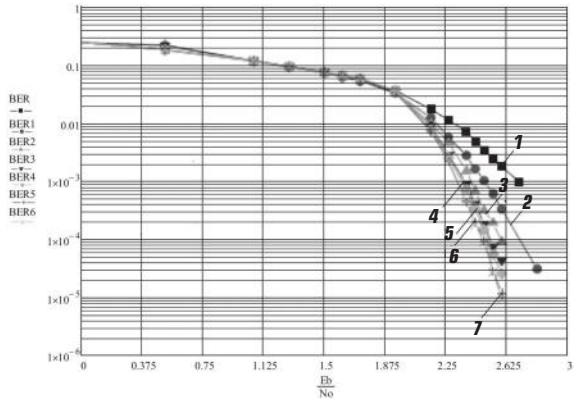


Рис. 14. Графіки залежності для оцінювання завадостійкості (BER) каскадної схеми зі змінною глибиною перемежування в разі СКК: ЗК (7, 1/2), РС(255, 223): *1* — $I = 1$; *2* — $I = 2$; *3* — $I = 3$; *4* — $I = 4$; *5* — $I = 5$; *6* — $I = 8$; *7* — $I = 16$

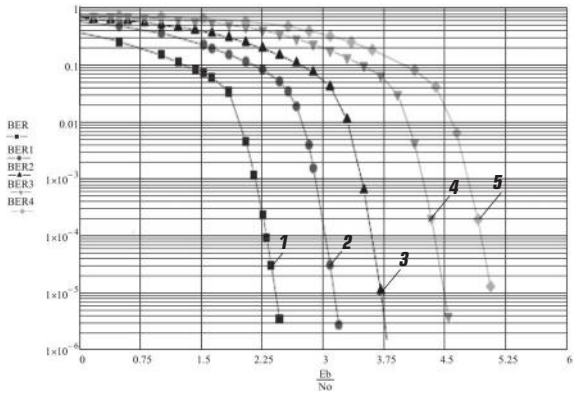


Рис. 15. Графіки для оцінювання завадостійкості (BER) каскадної схеми ($t = 16$) за СКК: РС (255, 223) і внутрішнього згорткового коду (глибина перемежування $I = 5$): *1* — ЗК (7, 1/2); *2* — ЗК (7, 2/3); *3* — ЗК (7, 3/4); *4* — ЗК (7, 5/6); *5* — ЗК (7, 7/8)

Під час дослідження встановлено, що глибина перемежування $I = 5$ дає значне наближення до ідеальної продуктивності в AWGN каналі.

Процес дослідження каскадної конструкції канального кодування здійснимо відповідно до схеми алгоритму, наведеної на рис. 16.

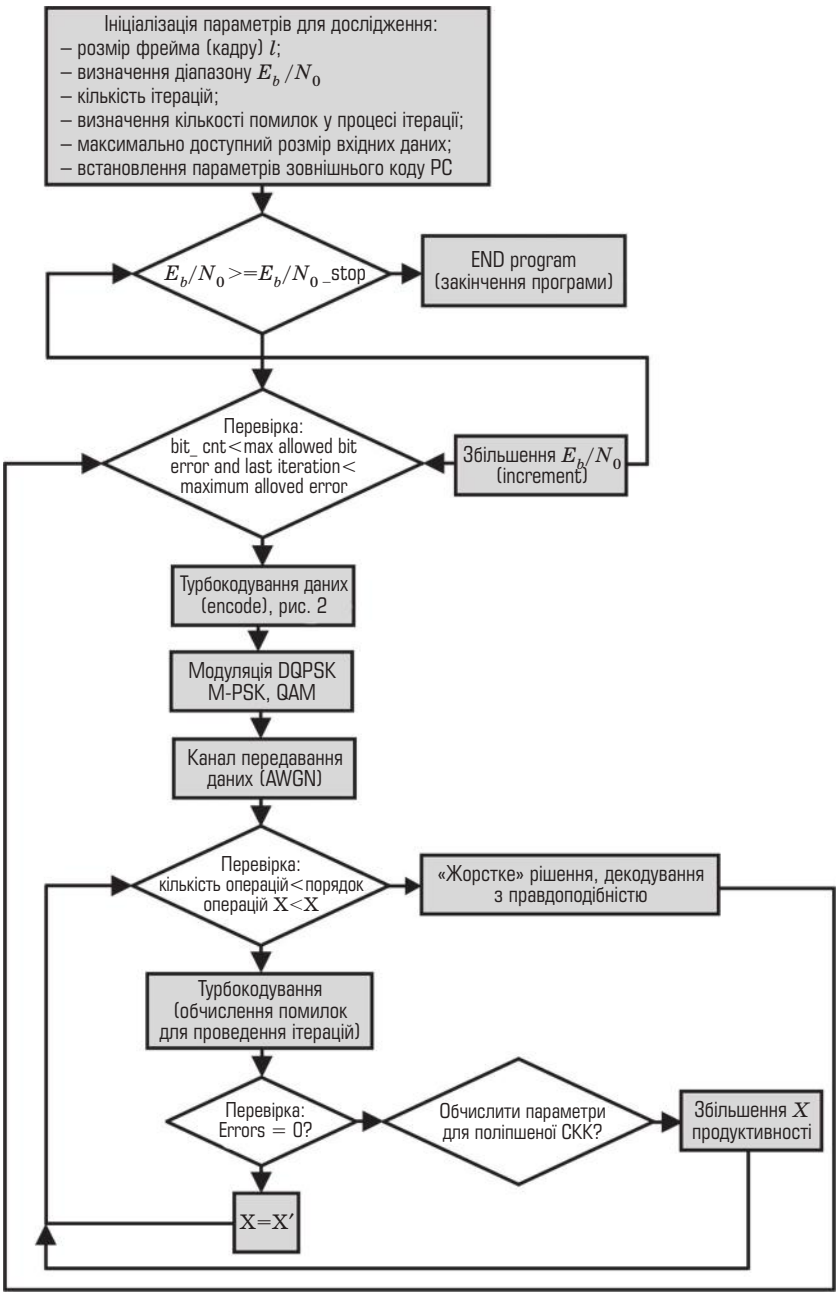


Рис. 16. Схема реалізації алгоритму дослідження каскадної конструкції канального коду

Імітаційну схему телекомунікаційної системи передавання інформації з каскадним кодуванням наведено на рис 17. Зовнішній кодер виконано за структурою кодера РС (255, 223), внутрішній — турбокодер ($R = 1/2$, і $R = 1/3$). Відповідно до схеми на рис. 16 симуляцію імітаційної схеми проводили шляхом ініціалізації параметрів та зміною кількості ітерації для описаних кодів. При формуванні каналу (див. рис. 17) використовували диференціальну квадратурну фазову маніпуляцію DQPSK. На приймальному боці застосовували декодер турбокоду з обчисленням апостеріорної ймовірності (APP) — рис. 18, *а*, а також систему синхронізації на основі модифікованої конструкції з передискретизацією сигналу [11–14]. Результати дослідження впливу кількості ітерацій при турбокодуванні на кількість правильно декодованих блоків подано на рис. 19, *а*. Згідно з рис. 19, *б* встановлюємо, що збільшення кількість ітерацій до 8 зменшує кількість хибно декодованих транспортних блоків. Зрештою всі помилки декодування, подані на рис. 19, *а*, відсутні.

Залежності завадостійкості при турбокодуванні від кількості ітерацій для каскадної СКК виду РС + ТК + DQPSK наведено на рис. 20, де подано також залежності для визначення енергетичного виграшу запропонованої СКК і СКК інших конструкцій.

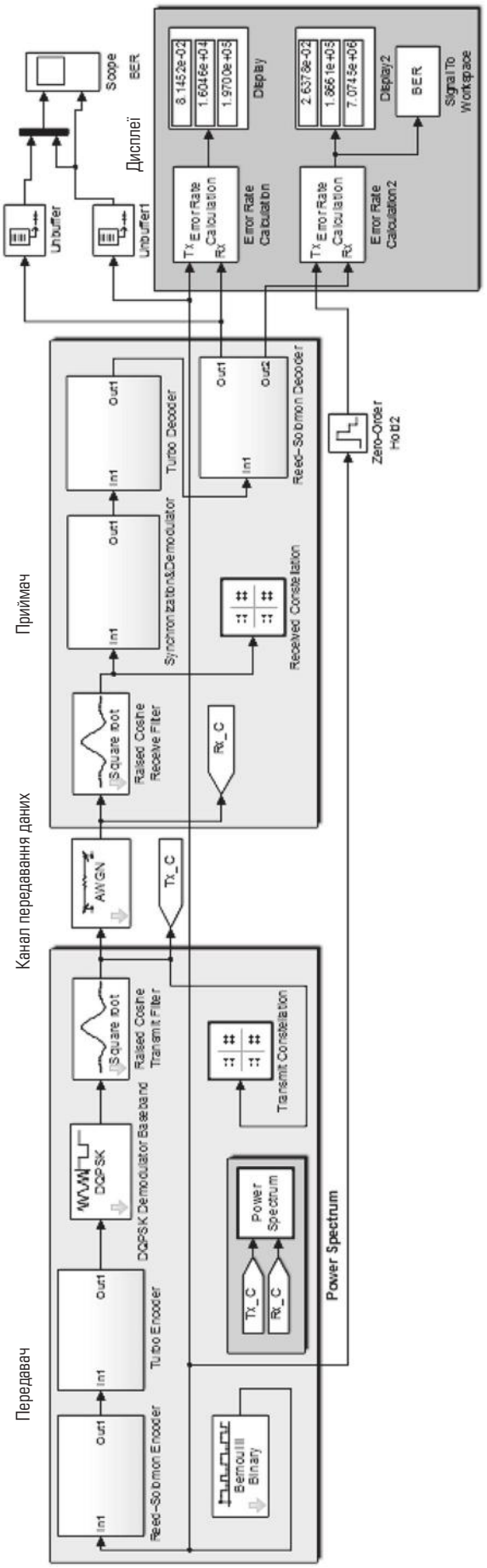


Рис. 17. Імітаційна схема телекомунікаційної системи передавання інформації з каскадним кодуванням

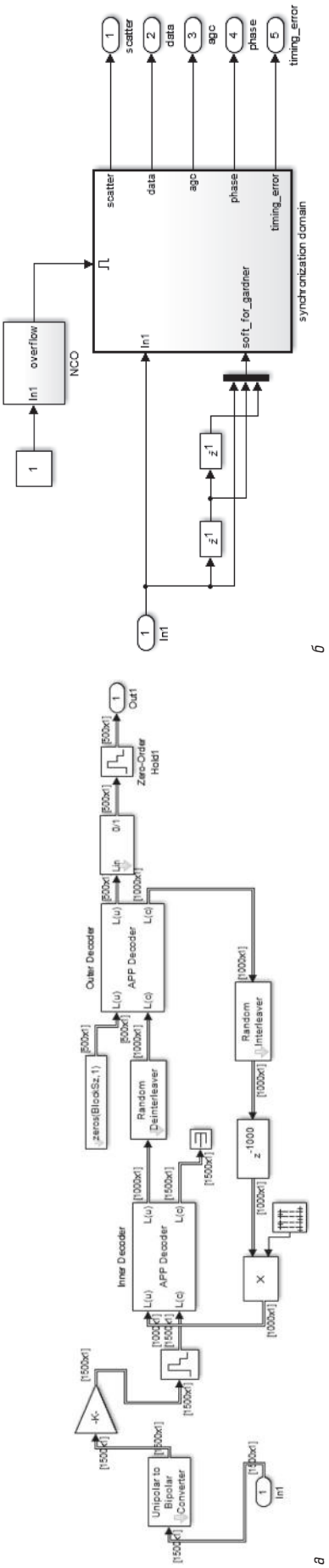
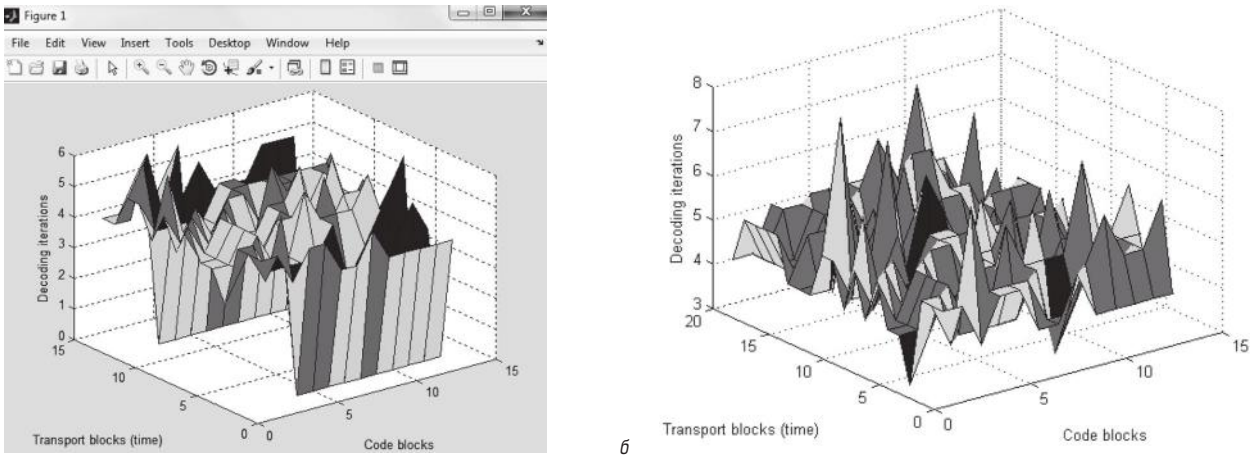
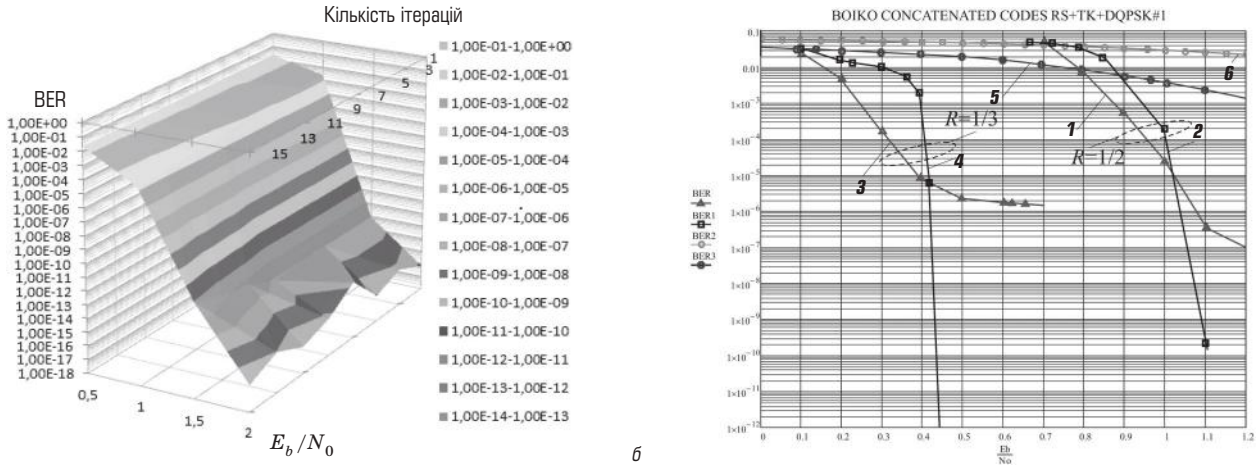


Рис. 18. Фрагменти імітаційних схем підсистем декодера турбокоду (*а*) та пристрою синхронізації (*б*)



а *б*

Рис. 19. Залежності кількості правильно декодованих транспортних блоків при турбокодуванні для різної кількості ітерацій: *а* — шість ітерацій; *б* — вісім ітерацій



а *б*

Рис. 20. Залежності завадостійкості при турбокодуванні для каскадної ССК виду РС (255, 239) + ТК (L = 16384 бітів; 10 ітерацій) + DQPSK: *а* — у разі зміни кількості ітерацій; *б* — у разі зміни енергетичного виграшу кодування при різних значеннях R: *1* — R = 1/2; *2* — R=1/2; *3* — R = 1/3; *4* — R = 1/3; *5* — РС(255, 239); *6* — некодована DQPSK

Висновки

1. Запропоновано схему реалізації телекомунікаційного каналу передавання даних на основі каскадної конструкції турбокодування з метою підвищення захищеності та завадостійкості за наявності завад.

2. Розроблено структуру складових кодів каскадної конструкції та описано принципи синхронізації і перемежування бітових даних при канальному кодуванні.

3. Наведено математичні моделі для формалізованого опису роботи складових каскадного коду. Запропонований, зокрема, вид породжувального полінома для канального кодування.

4. Як показали описані в статті дослідження, зростання кількості ітерацій при турбокодуванні підвищує ефективність результату. ЕВК для розглянутих ССК досягає 5,9 дБ.

5. Розроблено імітаційну схему та алгоритм телекомунікаційної системи з каскадним кодування на основі такої ССК: РС+ТК+ +DQPSK. Ця схема усунула ефект насичення ТК для запропонованих кодів та дозволила отримати ЕВК на рівні 3,1 дБ (BER = 10^{-8}).

У подальших дослідженнях увагу буде приділено визначенню поведінки запропонованих каскадних кодів вніслідок зміни ССК, а також особливостям використання багатопозиційної квадратурної амплітудно-фазової маніпуляції, дослідженню завадостійкості при зміні структури ТК складового каскадного коду, пошуку каскадного коду «прозорого» до спотворень фази вихідного сигналу в разі захищеної телекомунікаційної системи передавання інформації.

Література

1. ***Boiko, J. M.*** *Improvements Encoding Energy Benefit in Protected Telecommunication Data Transmission Channels. Communications / J. M. Boiko, A. I. Eromenko // Science Publishing Group, USA.— 2014.— Vol. 2, No. 1.— P. 7–14.*

2. ***Бойко, Ю. М.*** *Можливості турбокодів щодо підвищення енергетичного виграшу в каналах передавання інформації / Ю. М. Бойко // Зв'язок.— 2016.— №2.— С. 16–25.*

3. ***Boiko, J.*** *Improving noise immunity of QPSK demodulation of signals in digital satellite communication systems / Juliy Boiko, Victor Stetsiuk, Victor Michan // TCSET'2012 IEEE, Feb., Lviv – Slavsko.— P. 257.*

4. **Пятін, І. С.** *Дослідження фазових детекторів / І. С. Пятін // Вісник ХНУ. Технічні науки.— 2013.— №5.— С. 239–243.*

5. **Franceschni, M.** *LDPC coded modulations / M. Franceschni, G. Ferrari, R Raheli // Springer Dordrecht Heidelberg London New York – USA, 2009.— P. 195.*

6. **Банкет, В. Л.** *Сигнально-кодовые конструкции в телекоммуникационных системах / В. Л. Банкет.— О.: Феникс, 2009.— 180 с.*

7. **Бойко, Ю. М.** *Основи функціонування багатоканальних систем передачі інформації: навч. посіб. для ВНЗ / О. М. Шинкарук, Ю. М. Бойко, І. І. Чесановський.— Хмельницький: ХНУ, 2011.— 231 с.*

8. **Boiko, J. M.** *Noise immunity assessment in telecommunication systems with cascade encoding structures / J. Boiko, O. Eromenko //TCSET'2014 IEEE. 25 February – 1 March 2014.— Lviv – Slavske.— P. 431–433.*

9. **Boiko, J. M.** *Solutions Improve Signal Processing In Digital Satellite Communication Channels / J. M. Boiko, A. I. Eromenko // 20th International IEEE conference on microwaves, radar and wireless communications. MIKON-2014, June, Gdansk – Poland.— P. 126–129.*

10. **Boiko, J. M.** *Improving effectiveness for processing signals in data transmission channels with phase manipulation / J. M. Boiko // 23rd International IEEE Crimean Conference «Microwave & Telecommunication Technology», September 9–13, Sevastopol.— P. 262–263.*

11. **Shynkaruk, O.** *Measurements of the energy gain in the modified circuit signal processing unit / Oleg Shynkaruk, Juliy Boiko, Oleksander Eromenko // TCSET'2016 IEEE, Feb., Lviv – Slavsko.— P. 582–585.*

12. **Бойко, Ю. М.** *Проблеми синтезу пристроїв тактової синхронізації приймачів супутникових телекомунікаційних систем передачі інформації / Ю. М. Бойко, О. І. Єрьоменко // Вісник НТУУ КПІ. Телекомунікації, радіолокація і навігація, електроакустика.— 2014.— № 58.— С. 55–66.*

13. **Бойко, Ю. М.** *Підвищення завадостійкості блоків оброблення сигналів супутникових засобів телекомунікацій на основі модифікованих схем синхронізації /Ю. М. Бойко // Вісник НТУУ КПІ. Телекомунікації, радіолокація і навігація, електроакустика.— 2015.— № 61.— С. 91–107.*

14. **Бойко, Ю. Н.** *Моделирование устройства синхронизации на полифазном интерполяторе в средствах телекоммуникаций: сб. статей НИЦ «Знание» / Ю. Н. Бойко.— Харьков.— 2016.— Ч. 1.— С. 70–77.*

Рецензент: доктор техн. наук, професор **В. А. Дружинін**, Державний університет телекомунікацій, Київ.

Ю. Н. Бойко, Д. А. Макаришкин, А. И. Пасечник

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ КАНАЛЬНОГО КОДИРОВАНИЯ В ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

Рассмотрены механизмы повышения защищенности телекоммуникационных систем с применением алгоритмов помехоустойчивого канального кодирования. Сформирована структура канала передачи информации с турбокодированием. Рассмотрена блок-диаграмма кодера турбокода для формирования схемы защищенной телекоммуникационной системы. Формализованы принципы декодирования турбокода на базе итеративного декодера. Описаны подходы к синхронизации турбокодов с использованием специального прикрепленного маркера. Приведены экспериментальные данные для определения энергетического выигрыша кодирования для различных длин блоков турбокодов. Предложены и исследованы схемы реализации кодера с чередованием битов данных для составляющих кодов при реализации телекоммуникационной системы передачи информации с канальным кодированием. Описана фреймовая структура пакета данных для передачи информации кодом Рида–Соломона. Разработана имитационная схема телекоммуникационной системы передачи данных для исследования принципов формирования сигналов на основе каскадных кодов. Получены результаты применения указанной схемы в телекоммуникационных системах с каскадным кодированием в случае определения энергетического выигрыша и устранения эффекта насыщения турбокодов.

Ключевые слова: канальное кодирование; фазовая манипуляция; сигнально-кодовая конструкция; телекоммуникационная система.

J. M. Boiko, D. A. Makaryshkin, O. I. Pasichnyk

RESEARCH INTO EFFECTIVENESS OF CHANNEL CODING ALGORITHMS IN PROTECTED TELECOMMUNICATION INFORMATION TRANSMISSION SYSTEMS

In this paper represents the mechanisms more secure telecommunications systems through the use of algorithms for noise-immune channel coding. Formed channel structure information transmission with turbo coding (TK). Considered a block diagram of a turbo encoder code to create diagrams secure telecommunications system. Formalized principles decoding turbo codes using an iterative decoder. Describe the principles and implementation process synchronization turbo codes through the use of synchronization marker attached. The experimental data to determine the energy gain coding (EGC) for different lengths of blocks of turbo codes. Proposed and tested circuit implementation of encoder data bits interleaving codes for the components in the implementation of the telecommunications system with channel coding. Described frame structures for data packet transfer information code Reed–Solomon (RS). Developed simulation scheme for research principles of signals based on concatenated codes in telecommunication systems. The results of the simulation study scheme channel information transmission in telecommunication systems with concatenated encoding when determining the energy gain saturation effect and eliminate turbo codes. Studies conducted in the show, affects the number of iterations in the turbo coding efficiency increases result EGC considered for SCC was 5.9 dB. The developed algorithm and circuit simulation telecommunication system of the concatenated coding based CCM: RS + TC + DQPSK.

Keywords: channel coding; phase shift keying; signal-code construction; telecommunication system.