Міністерство освіти і науки України
Вінницький національний технічний університет

В. П. Семеренко

ТЕОРІЯ ЦИКЛІЧНИХ КОДІВ НА ОСНОВІ АВТОМАТНИХ МОДЕЛЕЙ

Монографія

Вінниця
ВНТУ
2015

УДК 681.3.06.(075)
ББК 32.973.26-018.1
С34

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 7 від 26.02.2015 р.)

Рецензенти:
В. А. Лужецький, доктор технічних наук, професор
Л. І. Тимченко, доктор технічних наук, професор

Семеренко, В. П.

С34 Теорія циклічних кодів на основі автоматних моделей : монографія / В. П. Семеренко. – Вінниця : ВНТУ, 2015. – 444 с.

ISBN 978-966-641-624-0

Запропоновані автоматні моделі циклічних кодів на основі теорії лінійних послідовнісних схем (ЛПС). Розглянуто систематичне і несистематичне кодування циклічних кодів за допомогою рекурсивних, нерекурсивних і комбінованих ЛПС. Наведені автоматно-графові методи декодування лінійної і поліноміальної складності для різних типів помилок: випадкових, пакетів помилок, стирань. Показані резерви підвищення продуктивності процедур кодування і декодування на основі паралельної обробки даних. Запропоновані нові оцінки здатності циклічних кодів виявляти та виправляти помилки на основі графового представлення коду. Розглянуті особливості кодів БЧХ, Ріда–Соломона, Файра, Абрамсона, і запропоновані паралельні циклічні коди.

УДК 681.3.06.(075)
ББК 32.973.26-018.1

ISBN 978-966-641-624-0

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АБГШ – канал з адитивним білим гаусівським шумом
БЧХ-код – код Боуза–Чоудхурі–Хоквінгема
ВОЛЗ – волоконно-оптична лінія зв’язку
ВПВ – «вертикальна» пов’язуюча вершина
ВПС – «вертикальний» пов’язуючий стан
ГПВП – генератор псевдовипадкової послідовності
ДКБП – дискретний канал без пам’яті
ДКС – двійковий канал зі стиранням
ДП – діаграма переходів
ДСК – двійковий симетричний канал
КЛ-код – квадратично-лишковий код
КДКС – комбінований двійковий канал зі стиранням
ЛПС – лінійна послідовнісна схема
ЛПМ – лінійна послідовнісна машина
М-послідовність – послідовність максимального періоду
МДВ-код – код з максимально досягнутою відстанню
НСК – найменше спільне кратне
НЦ – нульовий цикл
ОНЦ – основний нульовий цикл
ОЦ – одиничний цикл
ООЦ – основний одиничний цикл
ПВП – псевдовипадкова послідовність
ПНЦ – периферійний нульовий цикл
РД – решіткова діаграма
РЗЛОЗ – регістр зсуву з лінійним оберненим зв’язком
РС-код – код Ріда–Соломона
СА – сигнатурний аналізатор
ТОЦ – тривіальний одиничний цикл
ТНЦ – тривіальний нульовий цикл
ФГ – фактор-граф
ЦС – цифрова схема
CRC (Cyclic Redundancy Code) – циклічний надлишковий код

ПЕРЕДМОВА

Датою народження сучасного завадостійкого кодування прийнято вважати появу у 1948 році знаменитої статті К. Шеннона [1], в якій було доведено таке твердження (теорема Шеннона–Хартлі): при будь-якій продуктивності джерела повідомлень, що не перевищує пропускної здатності каналу, існує такий спосіб кодування, який дозволяє передати всю інформацію від джерела з довільно малою ймовірністю помилки.

Теорема не дає конкретних рекомендацій про способи побудови конкретних кодів для забезпечення ідеальної передачі інформації, однак саме ця обставина і стала початковим поштовхом до розвитку завадостійкого кодування.

Як і більшість інших фундаментальних відкриттів, роботи зарубіжних [2, 3] і вітчизняних [4, 5] піонерів в цій сфері науки з’явились у відповідь на практичні потреби. В 50-х і 60-х роках XX століття людство стало освоювати космічний простір і виникла необхідність в безпомилковій передачі даних від супутників та космічних кораблів [6].

Космічний зв'язок в ті роки мав свої особливості. По-перше, характер спотворень в таких каналах дуже точно описувався моделлю адитивного білого гаусового шуму, що спричинило вивчення саме таких теоретичних моделей каналів. Внаслідок великих відстаней для передачі даних були необхідні потужні коректувальні коди зі складними алгоритмами декодування, хоча платою за це була низька швидкість передачі корисних даних. Надлишок смуги пропуску дозволяв використовувати коди з низькою спектральною густиною.

Теорія завадостійкого кодування почала бурхливо розвиватися і поступово впроваджуватися в інші сфери: цифровий аудіо- та відеозв’язок, мобільний зв’язок і передачу даних в комп’ютерах. З кожним роком ставало все більш зрозумілим, що старі моделі вже не могли коректно описувати процеси в інших системах. Необхідність врахування різних системних і технологічних компромісів сприяла появі нових критеріїв оптимальності кодів.

Практичні потреби знову стали каталізатором подальшого розвитку завадостійкого кодування, яке продовжується і в наші дні. Значний внесок в розвиток теорії кодування внесли також і вчені України [7–13].

Не применшуючи значення численних відомих сьогодні кодів, все ж варто відзначити величезну роль завадостійких кодів, які входять до класу циклічних кодів. Вперше ці коди були запропоновані Прейнджем [14], а потім розвинуті в роботах учених, чиї імена увічнені в назвах досліджених ними кодів – Хемінга [2], Голея [3], Боуза і Рой-Чоудхурі [15], Хоквінгема [16], Файра [17], Ріда і Соломона [18].

Головними перевагами циклічних кодів є їх висока коректувальна здатність і прості схеми кодування–декодування. Саме тому вони мають дуже широку сферу використання: системи передачі даних, цифрове телебачення, магнітні і оптичні носії інформації. Прикладом одного з нових напрямків практичного застосування може служити організація захисту інформації в двовимірних матричних штрих-кодах за допомогою кодів Ріда–Соломона (РС) [19]. На основі циклічних кодів були розроблені коди Кердока, Препарати, Юстесена, Гоппи, альтернантні коди, алгеброгеометричні коди та інші.

В 60–80 роки з’явилися класичні роботи по кодуванню: У. Пітерсона, Ф. Мак-Вільямса, Н. Слоена, Е. Берлекемпа та інших зарубіжних та вітчизняних дослідників [20–29]. За останні два десятиріччя кращим виданням в цій області можна вважати енциклопедичну роботу Б. Скляра [30].

В кожній із зазначених книг є декілька розділів про циклічні коди. На жаль, практично відсутні серйозні роботи, які стосувалися б тільки циклічних кодів. Винятком може служити опублікована більше 40 років тому відома книга В. Д. Колесника і Е. Т. Мирончикова [31]. Недавно вийшла з друку нова книга В. Д. Колесника [32], де головну увагу приділено різноманітним підкласам циклічних кодів.

За минулий період з’явилося багато нових матеріалів, в яких досліджуються як традиційні циклічні коди, так і різні варіанти їх об’єднання з іншими кодами.

Тому давно з’явилась необхідність в узагальненні отриманих результатів і публікації нових книг, темою яких стали ці чудові коди.

Запропонована монографія направлена на ліквідацію вказаної прогалини.

Головною тенденцією в розвитку сучасних систем зв’язку є постійне збільшення швидкості передавання, практичне освоєння терабайтного діапазону. Основні досягнення останніх років пов’язані з широким використанням оптичних систем зв’язку [33]. Як і для попередніх технологій в системах передачі даних, основним резервом в підвищенні швидкості передавання є використання завадостійкого кодування. Використання кодів, що виправляють помилки (error correcting codes – ECC), дозволяє не тільки покращити якість передачі, але і зменшити кількість оптичних підсилювачів та збільшити довжину між регенераційними ділянками волоконно-оптичних ліній зв’язку (ВОЛЗ). [34]. Знаменним є те, що для наддалеких ВОЛЗ для швидкостей передавання 40 Гбіт/сек і вище вибір знову було зроблено на користь кодів РС. При високих відношеннях сигнал/шум послідовно з’єднані коди Боуза–Чоудхурі–Хоквінгема (БЧХ) і РС переважають недавно винайдені турбо-коди [35].

Однак, в оптичних системах передачі даних ще залишаються вузли електронної обробки і тому необхідна елементна база з граничними частотами, які щонайменше в п’ять разів перевищують швидкість передавання даних. Найкращим вирішенням цієї проблеми стане перехід до широкого використання паралельної обробки даних при кодуванні та декодуванні повідомлень.

Сучасні досягнення мікро- та наноелектроніки дозволяють апаратно й програмно реалізовувати складні алгоритми завадостійкого кодування й декодування з використанням кодів з великою коректувальною здатністю. Але швидке та ефективне виконання операцій кодоперетворення можливе тільки на основі принципів паралелізму. Завдяки паралельній обробці можна не тільки прискорити виконання традиційних процедур кодування–декодування, а також реалізувати нові підходи, наприклад, одночасний пошук помилок різних типів. Такі задачі актуальні для нестаціонарних каналів, в яких швидко змінюються параметри передачі даних.

Ще одним важливим резервом в підвищенні продуктивності при передачі даних є використання багатоканальних систем. Як

багатоканальні лінії зв’язку використовуються не тільки безпровідні, але і провідні лінії зв’язку (кабельний зв'язок). Найбільша сфера використання багатоканальних систем передачі даних – в комп’ютерах і комп’ютерних мережах [36, 37]. Їх головні особливості – інша модель помилок та словоорієнтована архітектура. Тому актуальною є розробка теоретичних основ паралельних циклічних кодів та ефективних методів їх кодування і декодування.

Для розв’язання нових задач необхідні розробка нових математичних моделей, нових методів обробки кодових сигналів, використання сучасних досягнень комп’ютерної архітектури з врахуванням специфіки паралельних обчислень.

Звичайно, автор не претендує на повноту викладення всіх аспектів, що пов’язані з циклічними кодами. Ця книга не є енциклопедією з циклічних кодів, в ній лише коротко наведені основні відомості про ці коди, а головна увага приділена новим результатам, які отримані автором: методам кодування й декодування циклічних кодів на основі їх автоматного представлення, розробці паралельних циклічних кодів в двійкових і недвійкових полях Галуа, а також використання методів паралельної обробки при програмній і апаратній реалізації кодерів–декодерів циклічних кодів.

REFERENCES

1. Shannon C. E. A mathematical theory of communication / C. E Shannon. – Bell Syst. Tech. J., 1948. – Vol. 27. – P. 379–423 (Part 1), P. 623–656 (Part 2). [Є переклад : Шеннон К. Работы по теории информации и кибернетике / К. Шеннон – М. : Изд-во иностр. лит., 1963. – 829 с.]

2. Hamming R. S. Error detecting and error correcting codes / R. S. Hamming. – Bell Syst. Tech. J. – 1950. – Vol. 29. – P. 147–160.

3. Goley M. J. T. Notes on digital codes / M. J. T. Goley // Proc. IRE, 1949. – Vol. 37. – P. 657.

4. Котельников В. А. Теория потенциальной помехоустой-чивости / В. А. Котельников. – М. : Госэнергоиздат, 1956. – 152 с.

5. Харкевич А. А. Очерки общей теории связи / А. А. Харкевич. – М. : Гостехиздат, 1955. – 270 с.

6. Applications of Error-Control Coding / [D. J. Costello, Jr., J. Hagenauer, H. Imai, S. B. Wicker]. // IEEE Trans. Inform. Theory. – 1998. – Vol. 44. – No. 6, – P. 2531–2560.

7. Кузьмин И. В. Основы теории информации и кодирования / И. В. Кузьмин, В. А. Кедрус. – 2-е изд. – К. : Вища школа, 1986. – 238 с.

8. Банкет В. Л. Цифровые методы в цифровой связи / В. Л. Банкет, В. М. Дорофеев. – М. : Радио и связь, 1988. – 240 с.

9. Белецкий А. Я. Преобразования Грея. Т. 1: Основы теории / А. Я. Белецкий, А. А. Белецкий, Е. А. Белецкий. – К. : НАУ, 2007. – 412 с.

10. Борисенко А. А. Биномиальное кодирование : монография / А. А. Борисенко, И. А. Кулик ; Сум. гос. ун-т. – Сумы : СумГУ, 2010. – 205 с.

11. Жураковський Ю. П. Теорія інформації та кодування: підручник / Ю. П. Жураковський, В. П. Полторак. – К. : Вища школа, 2001. – 255 с.

12. Лужецький В. А. Високонадійні математичні Фібоначчі-процесори: монографія / В. А. Лужецький. – Вінниця : УНІВЕРСУМ–Вінниця, 2000 р. – 248 с.

13. Стахов А. П. Коды золотой пропорции / А. П. Стахов. – М. : Радио и связь, 1984. – 152 с.

14. Prange E. Cyclic error-correcting codes in two symbols / E. Prange. – AFCRC-TN-57-103, Air Force Cambridge Research Center. Cambridge, Sept. 1957.

15. Bose R. C. On a class of error-correcting binary group codes / R. C. Bose, D. K. Ray-Chaudhuri. // Inf. Contr. – 1960. – Vol. 3. – P. 68–79.

16. Hocquenghem A. Codes correcteurs d’erreurs / A. Hocquenghem. – Chiffres, 1959. – T. 2. – P. 147–156

17. Fire P. A class of multiple-error correcting binary codes for nonindependent errors / P. Fire. – Sylvania Report RSL E-2, Sylvania Reconnaissance Systems Lab., Mountain View, Calif., 1959.

18. Reed I. S. Polynomial codes over certain finite fields / I. S. Reed, G. Solomon. – J. Soc. Indust. Appl. Math. – 1960. – Vol. 8. – P. 300–304.

19. ISO/IEC 18004 : 2006 Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification.

20. Питерсон У. Коды, исправляющие ошибки / У. Питерсон ; пер. с англ. – М. : Мир, 1964. – 340 с.

21. Берлекэмп Э. Алгебраическая теория кодирования / Э. Берлекэмп ; пер. с англ. – М. : Мир, 1971. – 477 с.

22. Мак-Вильямс Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн ; пер. с англ. – М. : Связь, 1979. – 744 с.

23. Касами Т. Теория кодирования / Т. Касами, Н. Токура, Ё. Ивадари, Я. Инагаки ; пер. с япон. – М. : Мир, 1978. – 576 с.

24. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут ; пер. с англ. – М. : Мир, 1986. – 576 с.

25. Кларк Дж., мл. Кодирование с исправлением ошибок в системах цифровой связи / Дж. Кларк мл., Дж. Кейн; пер. с англ. – М. : Радио и связь, 1987. – 392 с.

26. Галлагер Р. Теория информации и надежная связь / Р. Галлагер; пер. с англ. – М. : Сов. радио, 1974. – 719 с.

27. Кловский Д. Д. Передача дискретных сообщений по радио-каналам / Д. Д. Кловский – М. : Связь, 1969. – 375 с.

28. Финк Л. М. Теория передачи дискретных сообщений / Л. М. Финк. Изд. 2-е – М. : Советское радио, 1970. – 728 с.

29. Самойленко С. И. Помехоустойчивое кодирование / С. И. Самойленко. – М. : Наука, 1966. – 310 с.

30. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. ; Изд. 2-е, испр. ; Пер. с англ. – М. : Издательский дом «Вильямс», 2004. – 1104 с.

31. Колесник В. Д. Декодирование циклических кодов / В. Д. Колесник, Е. Т. Мирончиков. – М. : Связь, 1968. – 252 с.

32. Колесник В. Д. Кодирование при передаче и хранении информации (Алгебраическая теория блоковых кодов) / В. Д. Колесник. – М. : Высш. школа, 2009. – 550 с.

33. Слепов Н. Н. Современные технологии цифровых оптоволоконных сетей связи / Н. Н. Слепов. – Изд. 2-е, испр. – М. : Радио и связь, 2003. – 468 с.

34. Слепов Н. Н. Волоконные системы дальней связи. Перспективы развития / Н. Н. Слепов. // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. – 2005. – № 6 – С. 70–75.

35. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса ; пер. с англ. – М. : Техносфера, 2006. – 320 с.

36. Rao T. R. N. Error-Control Coding for Computer Systems / T. R. N. Rao, E. Fujiware. – Prentice Hall, Englewood Cliffs, N.Y., 1989.

37. Varsamou M. A new data allocation method for parallel probe-based storage devices / M. Varsamou, T. Antonakopoulos // IEEE Transactions on Magnetics. – 2008. – Vol. 44. – No. 4. – P. 547–554.

38. Прокис Дж. Цифровая связь / Дж. Прокис; пер. с англ. – М. : Радио и связь, 2000. – 800 с.

39. Блох Э. Л. Модели источники ошибок в каналах передачи цифровой информации / Э. Л. Блох, О. В. Попов, В. Я. Турин. – М. : Связь, 1971. – 312 с.

40. Богданов В. Н. Защита от ошибок в сетях АТМ / В. Н. Богданов, П. С. Вихлянцев, М. В. Симонов. // ИНФОРМОСТ. – 2002. – № 3 – С. 20–24.

41. Мелентьев О. Г. Теоретические аспекты передачи данных по каналам с группирующимися ошибками / О. Г. Мелентьев. – М. : Горячая линия-Телеком, 2007. – 232 с.

42. Березюк Н. Т. Кодирование информации (двоичные коды) / [Н. Т. Березюк, А. Г. Андрущенко, С. С. Мощицкий и др.]. – Харьков: Вища щкола, 1978. – 252 с.

43. G. D. Forney, Jr. Modulation and Coding for Linear Gaussian Channels / G. D. Forney, Jr., G. Ungerboeck. // IEEE Trans. Inform. Theory. – October, 1998. – Vol. 44. – No. 6. – P. 2384–2434.

44. Слепов Н. Н. Оценка показателей ошибок цифровых линий передачи / Н. Н. Слепов // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. – 2002. – № 5 – С. 22–28.

45. Васильев А. Н. Matlab. Самоучитель. Практический подход / А. Н. Васильев. – СПб. : Наука и техника, 2012. – 448 с.

46. Рекомендации МСЭ-Т G.821 (12/02). Показатели ошибок международного цифрового соединения, работающего на скорости передачи ниже первичной и образующего часть сети с интеграцией услуг.

47. Рекомендации МСЭ-Т G.826 (12/02). Параметры показателей ошибок и нормы между оконечными пунктами для международных цифровых трактов и соединений с постоянной скоростью передач.

48. Рекомендации МСЭ-Т G.828 (03/00). Параметры показателей ошибок и нормы для международных синхронных цифровых трактов с постоянной скоростью передач.

49. Рекомендации МСЭ-Т G.8201 (09/03). Параметры показателей ошибок и нормы между оконечными пунктами для международных трактов многих операторов в оптической транспортной сети многих операторов.

50. Лидл Р. Конечные поля. / Р. Лидл, Г. Нидеррайтер; в 2 т., Т. 1 – М. : Мир, 1988. – 430 с.

51. Фрид Э. Элементарное введение в абстрактную алгебру / Э. Фрид; пер. с венг. – М. : Мир, 1979. – 260 с.

52. Курош А. Г. Курс высшей алгебры / А. Г. Курош. ; Изд. 9-е. – М. : Наука, 1968. – 431 с.

53. Гилл А. Линейные последовательностные машины / А. Гилл ; пер. с англ. – М. : Наука, 1974. – 288 с.

54. Айчифер Э. С. Цифровая обработка сигналов: практический подход / Э. С. Айчифер, Б. У. Джервис. ; Изд. 2-е, испр. : пер. с англ. – М. : Издательский дом «Вильямс», 1992. – 992 с.

55. Кун С. Матричные процессоры на СБИС / С. Кун ; пер. с англ. – М. : Мир, 1991. – 672 с.

56. Friedland B. Linear Modular Sequential Circuits / B. Friedland // IRE Trans. – 1959. – Vol. 6. – P. 61–68.

57. Huffman D. A. The Syntsesis of Linear Sequential Coding Networks / D. A. Huffman. // Information Theory, Acad. Press Inc., N. Y., – 1956. – P. 77–95.

58. Huffman D. A. A Linear Circuit Viewpoint on Error-Correcting Codes / D. A. Huffman. // IRE Trans. – 1956. – Vol. IT-2. – P. 20–28.

59. Глушков В. М. Синтез цифровых автоматов / В. М. Глушков. – М. : Наука, 1966. – 476 с.

60. Кузнецов О. П. Дискретная математика для инженера / О. П. Кузнецов, Г. М. Адельсон-Вельский. ; Изд. 2-е. – М. : Энерго-атомиздат, 1988. – 480 с.

61. Фараджев Р. Г. Линейные последовательностные машины / Р. Г. Фараджев. – М. : Сов. радио, 1975. – 288 с.

62. Элспас Б. Теория автономных линейных последовательностных сетей / Б. Элспас // Киб. сборник.– М. : ИЛ., 1963. – Вып. 7. – С. 90–128.

63. Vardy A. Trellis Structure of Codes / A. Vardy, V. Pless, W. C. Huffman. Handbook of Coding Theory. – Eds, Amsterdam, The Netherlands : Elsevier, 1998.

64. Schlegel C. Trellis Coding / C. Schlegel. – New York : IEEE Press, 1997. – P. 274.

65. Tanner R. M. A Recursive Approach to Low Complexity Codes / R. M. Tanner // IEEE Trans. Inform. Theory. – Sep. 1981. – Vol. 27. – P. 533–547.

66. Gallager R. G. Low-Density Parity-Check Codes / R. G. Gallager. – Cambridge MA : MIT Press, 1963. – P. 90.

67. Wiberg N. Codes and Iterative Decoding on General Graphs / N. Wiberg, H. A. Loeliger, R. Kotter // Eur. Trans.Telecomm. – Sep./Oc. 1995. – Vol. 6. – P. 513–525.

68. Forney G. D. Codes on the graphs: Normal Realizations / G. D. Forney // IEEE Trans. Inform. Theory. – Fab. 2001. – Vol. 47. – P. 520–548.

69. Соловьева Ф. И. Введение в теорию кодирования: Учебное пособие / Ф. И. Соловьева. – Новосибирск : Новосибирский гос. ун-т, 2005. – 130 с.

70. Семеренко В.П. Разработка универсального кодера-декодера циклических кодов / В. П. Семеренко // Электронное моделирование. – 1995. – № 4. – С. 26–31.

71. Meggitt J. E. Error-correcting codes and their implementation / J. E. Meggitt // IRE Trans. Inf. Theory. – 1961. – Vol. IT-7. – P. 232–244.

72. Касами Т. Теория кодирования / Т. Кассами, Н. Токура, Е. Ивадари, Я. Инагаки ; пер. с япон. – М. : Мир, 1978. – 576 с.

73. Peterson W. W. Encoding and error-correction procedures for the Bose-Chaudhuri codes. / W. W Peterson // IEEE Trans. Inform. Theory. – 1960. – Vol. IT-6. – P. 459–470.

74. Gorenstein D. C. A class of error-correcting codes in p^m symbols. / D. C. Gorenstein, N. Zierler // J. Soc. Indust. Appl. Math. – 1961. – Vol. 9. – P. 207–214.

75. Massey J. L. Shift-register syntesis and BCH codes / J. L. Massey // IEEE Trans. Inform. Theory. – 1969. – Vol. IT-15. – P. 122–127.

76. Chien R. T. Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes. / R. T. Chien // IEEE Trans. Inform. Theory. – 1964. – Vol. 10. – P. 357–363.

77. Forney G. D., Jr. On decoding BCH codes. / G. D. Forney, Jr. // IEEE Trans. Inform. Theory. – 1965. – Vol. IT-11. – P. 549–557.

78. Coding Theory and Cryptography. The Essentials / [D. R. Hankerson, D. G. Hoffman, D. A. Leonard, C. C. Lindner, and others] Wall. Second Edition, Revised and Expanded. – New York : CRC Press. – 2000. – 350 p.

79. Золотарёв В. В. Теория и алгоритмы многопорогового декодирования / В. В. Золотарёв. – М. : Горячая линия-Телеком, 2006. – 270 с.

80. Omura J. K. A Probabilistic Decoding Algorithm for Binary Group Codes / J. K. Omura // Stanford Research Institute. Menlo Park, California, March 1969.

81. Семеренко В. П. Высокопроизводительные алгоритмы для исправления независимых ошибок в циклических кодах / В. П. Семеренко // Системи обробки інформації: зб. наук. пр. – Харків: ХУПС, 2010. – Вип. 3(84), – С. 80–89.

82. Prange E. The use of information sets in decoding cyclic codes / E. Prange // IRE Trans. Inf. Theory. – 1962. – Vol. IT-8.– P. 5–9.

83. Когновицкий О. С. Двойственный базис и его применение в телекоммуникациях / О. С. Когновицкий. – СПб. : Линк, 2009. – 411 с.

84. Конопелько В. К. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Изд. 3/ В. К. Конопелько, В. А. Липницкий. – М. : Едиториал УРСС, 2012. – 176 с.

85. Миллер Р. Последовательные и параллельные алгоритмы: Общий подход / Р. Миллер, Л. Боксер ; пер. с англ. – М. : БИНОМ. Лаборатория знаний, 2006. – 406 с.

86. Коричнев Л. П. Статистический контроль каналов связи / Л. П. Коричнев, В. Д. Королев. – М. : Радио и связь, 1989. – 240 с.

87. Abramson N. M. A class of Systematic Codes for Non-Independent Errors / N. M. Abramson // IRE Trans. Inf. Theory. – 1959. – Vol. IT-5. – No. 12. – P. 150–157.

88. Столлингс В. Компьютерные системы передачи данных / В. Столингс. ; Изд. 6-е; пер. с англ. – М., Издательский дом «Вильямс», 2002. – 928 с.

89. Вернер М. Основы кодирования. Учебник для вузов / М. Вернер ; пер. с англ. – М. : Техносфера, 2004. – 288 с.

90. Koopman P. Cyclic Redundancy Code (CRC) Polynomial Selection For Embedded Networks / P. Koopman, T. Chakravarty // The International Conference on Dependable Systems and Networks (DSN-2004). – June 2002. – P. 1–10.

91. Горяшко А. П. Синтез диагностируемых схем вычислительных устройств / А. П. Горяшко. – М. : Наука, 1987. – 288 с.

92. Reiger S. H. Codes for the correction of «clustered» errors / S. H. Reiger // IRE Trans. Inf. Theory, – Vol. 6. – Mar. 1960. – P. 16–21.

93. Семеренко В. П. Декодирование пакетов ошибок в циклических кодах / В. П. Семеренко // Математические машины и системы. – 1999. №1. – С. 30–48.

94. Semerenko V. P. Burst-Error Correction for Cyclic Codes / V. P. Semerenko // Proceeding of International IEEE Conference EUROCON2009, S. Petersburg, Russia. – P. 1646–1651.

95. Закревский А. Д. Логические уравнения / А. Д. Закревский ; Изд. 2-е. – М. : УРСС, 2003. – 95 с.

96. Fossorier M. Universal burst error correction / M. Fossorier // Proc. IEEE Int. Symp. Information Theory, Seatle, WA, Jul. 2006. – P. 1969–1973.

97. Berlecamp E. On the inherent intractability of certain coding problems / E. Berlecamp, R. J. McEliece, H. C. van Tilborg // IEEE Trans. Inform. Theory. – May, 1978. – Vol. 24. – No. 5. – P. 384–386.

98. Vardy A. The Intractability of Computing the Minimum Distance of a Code / A. Vardy // IEEE Trans. Inform. Theory. – November, 1997. – Vol. 43. – No. 1. – P. 1757–1766.

99. Dumer I. Hardness of Approximating the Minimum Distance of a Linear Code / I. Dumer, D. Micciancio, M. Sudan // IEEE Trans. Inform. Theory. – January, 2003. – Vol. 49. – No. 1. – P. 22–37.

100. Hartmann C. Generalizations of the BCH Bound / C. Hartmann, K. Tzeng // Information and Control. – 1972. – Vol. 20. – No. 5. – P. 489–498.

101. Roos C. A Generalization of the BCH Bound for Cyclic Codes, Including the Hartmann-Tzeng Bound Journal of Combinatorial Theory / C. Roos // Journal of Combinatorial Theory, Series A. – 1982. – Vol. 33. – No. 2. – P. 229–232.

102. Boston N. Bounding Minimum Distances of Cyclic Codes Using Algebraic Geometry / N. Boston // Electronic Notes in Discrete Mathematics. – 2001. –Vol. 6. – No. 5. – P. 384–386.

103. van Lint, J. H. On The Minimum Distance of Cyclic Codes / J. H. van Lint, R. M. Wilson // IEEE Transactions on Information Theory. – 1986. – Vol. 32. – No. 1. – P. 23–40.

104. Семеренко В. П. Оценка корректирующей способности циклических кодов на основе автоматных моделей / В. П. Семеренко //

Східно-європейський журнал передових технологій. – 2015. – № 2. – С. 16–24.

105. Конопелько В. К. Анализ возможности применения БЧХ кодов для коррекции зависимых ошибок / В. К. Конопелько, О. Г. Смолякова, А. В. Шкиленок // Доклады БГУИР. – 2007. – № 5. – С. 17–22.

106. Теория электрической связи. Учебное пособие / [К. К. Васильев, В. А. Глушков, А. В. Дермидонтов, А. Г. Нестеренко]. – Ульяновск. : УлГТУ, 2008. – 452 с.

107. Lin S. Error-Control Coding: Fundamentals and Applications / S. Lin, D. J. Costello ; 2nd. ed. – Upper Saddle River, NJ : Prentice-Hall, 2004.

108. Форни Д. Каскадные коды / Д. Форни ; пер. с англ. – М. : Мир, 1970. – 207 с.

109. Шахнович И. DVB-T2 – новый стандарт цифрового телевизионного вещания/ И. Шахнович // Электроника: НТБ. – 2009. – № 6. – С. 30–35.

110. Блох Э. Л. Обобщенные каскадные коды / Э. Л. Блох, В. В. Зяблов. – М. : Связь, 1976. – 240 с.

111. Guruswami V. Maximum-likelihood decoding of Reed-Solomon codes is NP-hard ECCC / V. Guruswami, A. Vardy. – Rep. TR 04-40. – Apr. 2004.

112. Jiang Gross J. Algebraic soft-decision decoding of Reed-Solomon codes using bit-level soft information / J. Jiang Gross, K. R. Narayanan // IEEE Trans. Inform. Theory. – Sep. 2008. – Vol. 54. – No. 9. – P. 3907–3928.

113. Welch L. R. Error Correction for Algebraic Block Codes / L. R. Welch, E. R. Berlecamp, U.S.A. – No. 4 633 470. Dec., 30, 1986.

114. Sudan M. Decoding of Reed-Solomon beyond the error-correction bound / M. Sudan, // J. Complexity. – Sep. 1997. – Vol. 13. – P. 180–193.

115. Guruswami V. Improved decoding of Reed-Solomon and algebraic-geometry codes / V. Guruswami, M. Sudan // IEEE Trans. Inform. Theory. – Sep. 1999 Vol. 45. – No. 6. – P. 1757–1767.

116. Wu Y. New list decoding algorithms for Reed-Solomon and BCH Codes / Y. Wu // IEEE Trans. Inform. Theory. – Aug. 2008. – Vol. 54. – No.8. – P. 3611–3630.

117. Семеренко В. П. Декодирование кодов Рида–Соломона на основе графовой и автоматной моделей / В. П. Семеренко // Электронное моделирование. – 2011. – № 1. – С. 57–72.

118. Chen G. A Burst-error Algorithm for Reed-Solomon Codes / G. Chen, P. Owsley // IEEE Trans. Inform. Theory. – Nov. 1992. – Vol. 38. – No. 6. – P.1807–1812.

119. Metzner J. J. On Correcting Bursts (and Random Errors) in Vector Symbol (n, k) Cyclic Codes / J. J. Metzner // IEEE Trans. Inform. Theory. – April, 2008. – Vol. 54. – No. 4. – P. 1795–1807.

120. Semerenko V. P. On Correcting of the Full Burst Errors for Reed–Solomon Codes / V. P. Semerenko // STATISTICAL METHODS OF SIGNAL AND DATA PROCESSING (SMSDP-2010) : Proceedings. Kiev, Ukraine, October 13–14. – 2010. – P. 169–171.

121. Семеренко В. П. Параллельное декодирование укороченных циклических кодов / В. П. Семеренко // Оптико-электронные информационно-энергетические технологии. – 2012. – № 1. – С. 30–41.

122. Казаков М. А. Разработка логики визуализаторов алгоритмов на основе конечных автоматов: / М. А. Казаков, Г. А. Корнеев, А. А. Шалыто. Телекоммуникации и информатизация образования. – 2003. – № 6. – С. 27–58.

123. Семеренко В. П. Паралельні алгоритми завадостійкого кодування / В. П. Семеренко // European Conference on Innovations in Technical and Natural Sciences. Proceedings of the 1st International scientific conference (February 17, 2014). «East West» Association for Advanced Studies and Higher Education GmbH. Vienna. 2014. – P. 82–88.

124. Хокинг С. Краткая история времени: От Большого взрыва до черных дыр / С. Хокинг ; пер. с англ. – СПб. : Амфора, 2008. – 231 с.

125. Пригожин И. Время, хаос, квант / И. Пригожин, И. Стенгерс. – М. : Издат. группа Прогресс, 1994. – 272 с.

126. Логика. Автоматы. Алгоритмы / [М. А. Айзерман, Л. А. Гусев, Л. И. Розоноэр, И. М. Смирнова, А. А. Таль]. – М. : Физматгиз, 1963. – 556 с.

127. Семеренко В. П. Темпоральні моделі паралельних обчислень / В. П. Семеренко // Austrian Journal of Technical and Natural Sciences. – January-February, 2014. – № 1. – P. 13–25.

128. Габидулин Э. М. Кодирование в радиоэлектронике / Э. М. Габидулин, В. Б. Афанасьев. – М. : Радио и связь, 1986. – 176 с.

129. Viswanath P. Opportunistic Beam Forming Using Dumb Antennas / P. Viswanath, N. David C. Tse, R. Laroia // IEEE Trans. Inform. Theory. – Juny 2002. – Vol. 52. – P. 1277–1294.

130. Конопелько В. К. Надежное хранение информации в полупроводниковых запоминающих устройствах: / В. К. Конопелько, В. В. Лосев. – М. : Радио и связь, 1986. – 240 с.

131. Hsiao M. Y. Single-Channel Error Correction in an f-Channel System / M. Y. Hsiao // IEEE Trans. On Computers. – Oct. 1968. – Vol. 17. – P. 935–943.

132. Ahlswede R. Multi–way communication channels / R. Ahlswede // 2nd Int. Symp. Inform. Theory, 23–52, Publishing House of the Hungarian Academy of Sciences. Tsahkadzor, Armenian SSR, 1973.

133. Fujiwara E. Parallel Decoding for Burst Error Control Codes / E. Fujiwara, K. Namba, M. Kitakami // Electronics and Comm. in Japan. – Jan. 2004. – Vol. 87. – No. 1. – P. 38–48.

134. Семеренко В. П. Паралельні циклічні коди / В. П. Семеренко // Вісник ВПІ. – 2014. – № 6. – С. 65–72.

135. Патент на корисну модель «Пристрій для виправлення помилок в циклічних (n, k)-кодах» / Семеренко В. П. – № 93798; заявл. 29.05.2014 ; опубл. 10.10. 2014, Бюл. № 19.

136. McEliece R. J. A Public-Key Criptosystem Based on Algebraic Theory / R. J. McEliece // DGN Progres Report 42–44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114–116.

137. Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory / H. Niederreiter // Probl. Control and Inform. Theory. – 1986. – Vol. 15. – P. 19–34.

138. Конопелько В. К. Защита информации кодовыми криптосистемами на основе теории норм синдромов и свойств циклотомической перестановки чисел / В. К. Конопелько, О. Г. Смолякова. // Технические средства защиты информации. Материалы докл. 6-й Белорусско-российской научно-техн. конф. (Минск 19–23 мая 2008 г.). – Минск. – С. 65.

139. Сидельников В. М. Открытое шифрование на основе двоичных кодов Рида–Маллера / В. М. Сидельников // Дискретная математика. – М., 1994. – Том 6, Вып. 3. – С. 3–20.

140. Стасев Ю. В. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов / Ю. В. Стасев, А. А. Кузнецов // Кибернетика и системный анализ. – 2005. – № 3. – С. 47–57.

141. Осмоловский С. А. Стохастические методы защиты информации / С. А. Осмоловский. – М. : Радио и связь, 2003. – 320 с.

142. Кириллов С. Н. Модифицированный помехозащищенный кодер на основе БИХ-фильтра / С. Н. Кириллов, Д. С. Семин // Вестник РГРТУ. – Рязань, 2009. – № 2 (Вып. 28). – С. 27–30.

143. Семеренко В. П. Потокове шифрування на основі теорії лінійної послідовнісної машини / В. П. Семеренко,
Ю. В. Степанишин, М. Л. Гаєвський // Інформаційні технології та комп‘ютерна інженерія. – 2007. – № 3 – С. 86–93.

144. Семеренко В. П. Интегрированная защита информации: криптография плюс помехоустойчивое кодирование / В. П. Семеренко // Захист інформації, 2011. – № 3. – С. 44–52.

145. Аграновский А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади – М. : СОЛОН-Пресс, 2002. – 256 с.

146. Логачев О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко – М. : МЦНМО, 2004. – 470 с.

147. Поточные шифры / [А. В. Асосков, М. А. Иванов, А. А. Мирский и др.]. – М. : КУДИЦ-ОБРАЗ, 2003. – 336 с.

148. Семеренко В. П. Разработка хэш-функции на основе поточного шифрования / В. П. Семеренко, П. В. Ширшова // Защита информации : сборник научных трудов НАУ, Вып. 15. – К. : НАУ, 2008. – С. 163–166.

149. Impagliazzo R. Pseudo-random generation from one-way functions / R. Impagliazzo, L. Levin, M. Luby // Proc. 21st Annu. ACM Symp. on Theory of Computing. – 1989. – P. 12–24.

150. Hastad J. Pseudo-random generators under uniform assumptions // Proc. 22nd Annu. ACM Symp. on Theory of Computing. 1990.
P. 395–404.

151. Ярмольник В. Н. Контроль и диагностика цифровых узлов ЭВМ / В. Н. Ярмольник. – Минск : Наука и техника, 1988. – 240 с.

152. Щербаков Н. С. Достоверность работы цифровых устройств информации / Н. С. Щербаков – М. : Машиностроение, 1989. – 224 с.

153. Савченко Ю. Г. Цифровые устройства, нечувствительные к неисправностям элементов информации / Ю. Г. Савченко – М. : Советское радио, 1977. – 176 с.

154. Дяченко О. Н. Компактное тестирование запоминающих устройств с локализацией пакетов ошибок / О. Н. Дяченко // Электронное моделирование. – 1996. – № 6. – С. 43–48.