ХАРЬКОВСКИЙ УНИВЕРСИТЕТ ВОЗДУШНИХ СИЛ
ИМЕНИ ИВАНА КОЖЕДУБА
г. Харьков, ул. Сумская, 77/79

На правах рукописи
УДК 621.391 (0.43)

Пасько Игорь Владимирович

МЕТОДЫ ПОСТРОЕНИЯ ЛИНЕЙНЫХ БЛОКОВЫХ КОДОВ С УЛУЧШЕННЫМИ СВОЙСТВАМИ ДЛЯ ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ ПЕРЕДАЧИ ДИСКРЕТНЫХ СООБЩЕНИЙ

Специальность: 05.12.02
«Телекоммуникационные системы и сети»

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
кандидат технических наук,
старший научный сотрудник
Кузнецов Александр Александрович

Харьков – 2008

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Одним из главных стратегических приоритетов государственной политики Украины в сфере науки и техники, утвержденных Постановлением Верховной Рады Украины, есть развитие перспективных информационных технологий, приборов автоматизации и систем связи [2, 3, 21, 22, 27, 30, 40, 63, 90]. В соответствии с Законом Украины "О Концепции Национальной программы информатизации", одним из основных направлений информатизации есть информатизация стратегических направлений развития государственности, безопасности и обороны [1, 2, 3, 21, 26, 30, 40, 73, 74, 90]. Главной особенностью задач этого направления является высокая сложность, обусловленная высокими требованиями к скорости и форме предоставления информации, помехоустойчивости и безопасности передачи дискретных сообщений в телекоммуникационных системах и сетях [7, 29, 31, 48, 81, 91, 96, 110].

Основными приоритетами в развитии телекоммуникационных систем и сетей Украины являются [16, 40, 74, 80, 87, 90]: исследование, разработка и внедрение новых принципов организации связи; создание средств связи, которые будут способствовать ускорению развития и повышению эффективности телекоммуникационных систем и сетей; организация разработки и производства в Украине основных видов технических средств и необходимых компонентов телекоммуникаций на уровне европейских и мировых стандартов качества [23, 29, 31, 40, 44, 48, 74, 80, 87, 90]. Современный технологический уровень разработки и производства средств связи невозможно обеспечить без проведения упреждающих исследований, а организацию внедрения передовых технологий и новейшей техники – без постоянного сопровождения этих процессов отраслевой наукой.

Основы научного подхода к построению цифровых систем связи заложены в работах известного американского ученого Клода Шеннона

[108, 109], который математически формализовал процессы цифровой обработки сообщений, впервые ввел и теоретически обосновал количественную меру информации как меру неопределенности, а также ввел понятие ненадежности канала связи как меру средней неопределенности принятого сигнала при наличии шума. В фундаментальной работе «Математическая теория связи» К. Шеннон доказал возможность передачи сообщений по каналу с шумом со сколь угодно малой вероятностью ошибки при условии применения специальных систем кодирования и при скорости передачи сообщения, меньшей пропускной способности канала [109]. Другими словами, им было установлено, что вероятность ошибочного приема сообщений является функцией сложности кодирования, а не функцией скорости передачи сообщений. Этот замечательный вывод дал значительный толчок в развитии нового научного направления (теории помехоустойчивого кодирования), основной задачей которого является поиск вычислительно эффективных методов кодирования для передачи дискретных сообщений с малой вероятностью ошибки. К сожалению, на сегодняшний день эта проблема, в виду ее высокой сложности, далека от полного разрешения [75, 94, 122].

Актуальность темы.

Наибольшее развитие в теории помехоустойчивого кодирования получили методы и алгоритмы построения линейных блоковых кодов [4, 6, 8, 12, 16, 32, 41, 50, 94, 124, 130]. Используя развитый математический аппарат линейной алгебры и, в особенности, аппарат теории колец многочленов от одной формальной переменной в работах [4, 12, 17, 28, 36, 46, 68, 75, 94] развита теория построения циклических кодов – одного из наиболее крупных разделов современной теории помехоустойчивого кодирования. Наряду с высокими конструктивными свойствами циклических кодов этот подход позволяет строить простые и вычислительно эффективные алгоритмы кодирования и декодирования. Наибольший практический интерес в этом

смысле представляют коды Боуза-Чоудхури-Хоквингема (БЧХ коды), сложность алгебраического декодирования которых растет полиноминально от параметров кода [4, 69, 75, 94,]. Известно [6, 60, 62, 63, 74, 75], что алгоритм Берлекэмпа-Месси содержит число умножений, порядка t^2, или, формально, сложность алгоритма $O(t^2)$, где t – исправляющая способность кода. Таким образом, циклические коды и, в частности, коды БЧХ обладают на сегодняшний день вычислительно эффективными алгоритмами построения. В тоже время их практическое использование при больших длинах кодового слова не позволяет существенно повысить энергетическую эффективность передачи дискретных сообщений. Это объясняется плохими асимптотическими свойствами данного класса кодов. Практически, весь обширный класс циклических кодов при длине > 1000 символов для исправления ошибок не используется, передача сообщений в этих условиях энергетически не выгодна [47, 54, 90, 128].

Теоретическим обобщением алгебраических кодов, допускающих полиномиальное описание многочленами от одной формальной переменной, есть коды, ассоциированные с алгебраическими кривыми (алгеброгеометрические коды) [60, 74, 93, 114]. В работах [14, 63, 74, 107, 115] показано, что данный класс линейных блоковых кодов обладает существенным преимуществом – ассмиптотически алгеброгеометрические коды по своим параметрам лежат выше нижней кодовой границы Варшамова-Гилберта. Другими словами, применение данного класса кодов потенциально может привести к достижению показателей энергетической эффективности, близких к предельным оценкам К.Шеннона. В тоже время, на сегодняшний день методы построения и декодирования алгеброгеометрических кодов исследованы для плоских алгебраических кривых, заданных в проективном пространстве P^2 неприводимым однородным уравнением от трех переменных [47, 55, 56, 57, 62]. Этот подход позволяет строить простые схемы кодирования и декодирования

алгеброгеометрических кодов, длина которых над конечным полем *GF(q)* не превышает числа точек плоской кривой [22, 58, 74]. Перспективным направлением в этом смысле является разработка методов построения алгеброгеометрических кодов большой длины, например, кодов на пространственных кривых, задаваемых в проективном пространстве P^3 совместными решениями двух однородных уравнений от четырех переменных. Решение этой задачи позволит строить длинные недвоичные коды, с кодовыми характеристиками, лежащими выше границы Варшамова-Гилберта. Их практическое использование позволит повысить энергетическую эффективность передачи сообщений по каналам с шумом, что при фиксированной вероятности ошибочного приема символа сообщения позволит снизить требования к минимально необходимому соотношению энергии сигнала к спектральной плотности шума, т.е. повысить помехоустойчивость передачи дискретных сообщений.

Таким образом, развитие методов и алгоритмов построения алгеброгеометрических кодов на пространственных кривых является перспективным направлением исследований, имеющим важное значение как для развития отдельного направления теории помехоустойчивого кодирования, так и для решения прикладных вопросов помехоустойчивой передачи сообщений по каналам со случайно возникающими ошибками, тема диссертационного исследования является актуальной.

Связь работы с научными программами, планами, темами. Исследования в диссертационной работе проводились в соответствии со следующими нормативными актами.

1. Концепция развития связи Украины до 2010 года, утвержденная постановлением Кабинета Министров Украины «Про Концепцію розвитку зв'язку України до 2010 року» от 9 декабря 1999 г. №2238.

2. Концепция Национальной программы информатизации, одобренной Законом Украины «Про Концепцію Національної програми інформатизації» от 4 февраля 1998 г. N 75/98-ВР.
3. Государственная научно-техническая программа «Створення перспективних телекомунікаційних систем і технологій».
4. Тактико-техническое задание на научно-исследовательскую работу «Розробка методів підвищення якості військового зв’язку автоматизованої системи управління ракетних військ і артилерії», шифр «Мрія».
5. Тактико-техническое задание на научно-исследовательскую работу на специальную тему, шифр «Облік».
6. Тактико-техническое задание на опытно-конструкторскую работу «Створення УКХ радіостанцій, що забезпечують енергетично скритний та перешкодозахищений радіозв'язок у повнозв'язаній мережі».

Цель и задачи исследований. Целью диссертационной работы является повышение помехоустойчивости передачи дискретных сообщений на основе использования линейных блоковых кодов с улучшенными свойствами.

В соответствии с целью работы необходимо решить **научную задачу**, состоящую в разработке методов построения линейных блоковых кодов с улучшенными свойствами для повышения помехоустойчивости передачи дискретных сообщений.

Для достижения поставленной цели необходимо решить следующие **частные задачи**.

1. Провести анализ состояния и обосновать пути развития методов кодирования для повышения помехоустойчивости передачи дискретных сообщений.
2. Разработать метод и алгоритмы помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых для повышения помехоустойчивости передачи дискретных сообщений.

3. Разработать алгебраический метод и алгоритм декодирования алгеброгеометрических кодов на пространственных кривых для повышения помехоустойчивости передачи дискретных сообщений.
4. Исследовать помехоустойчивость передачи дискретных сообщений с использованием алгеброгеометрических кодов на пространственных кривых.

Объект исследования. Процесс помехоустойчивой передачи дискретных сообщений по каналам со случайно возникающими ошибками.

Предмет исследования. Методы построения линейных блоковых кодов с улучшенными свойствами для повышения помехоустойчивости передачи дискретных сообщений.

Методы исследования. При разработке методов и алгоритмов построения и декодирования линейных блоковых кодов с улучшенными свойствами использованы методы алгебраической теории блоковых кодов и теории информации, а так же методы теории алгебраических кривых и теории конечных полей Галуа. При разработке практических предложений по аппаратной реализации алгоритмов кодирования и декодирования использованы методы теории автоматов и теории сложности. При исследовании помехоустойчивости передачи дискретных сообщений использованы методы статистической теории связи, теории вероятности и математической статистики.

Научная новизна полученных результатов обусловлена теоретическим обобщением и новым решением научно-технической задачи, состоящей в разработке методов построения линейных блоковых кодов с улучшенными свойствами для повышения помехоустойчивости передачи дискретных сообщений.

Получены следующие **научные результаты**.

1. **Впервые получены** новые кодовые конструкции помехоустойчивых кодов как линейных систем возникающих на пространственных кривых,

отличающиеся от известных тем, что при фиксированной мощности алфавита и без ухудшения кодовых соотношений удается построить линейные блоковые коды большей длины [53, 55, 56].

2. **Получили дальнейшее развитие** методы помехоустойчивого кодирования недвоичными блоковыми кодами, возникающими на алгебраических кривых. Разработан метод кодирования алгеброгеометрическими кодами на пространственных кривых, отличающийся от известных формированием базиса линейного кода через отображение множества совместных решений двух однородных алгебраических уравнений от четырех переменных, что позволяет при фиксированной мощности алфавита символов и при сохранении высоких конструктивных кодовых характеристик получить бóльшую длину кода [22, 56].
3. **Усовершенствованы** методы декодирования недвоичных блоковых кодов, возникающих на алгебраических кривых. Разработан алгебраический метод декодирования алгеброгеометрических кодов на пространственных кривых, который отличается от известных формированием трехвариантного уравнения локаторов ошибок, решения которого однозначно задаются произошедшими ошибками, что позволяет свести задачу декодирования к решению системы линейных уравнений, у которых число неизвестных определяется конструктивными кодовыми характеристиками [55, 79, 80].

Практическое значение результатов диссертационных исследований состоит в следующем.

1. Выработаны практические рекомендации по реализации предложенных методов помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых. Разработаны алгоритмы и структурные схемы устройств помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых. Показано,

что формирование кодовых слов реализуется с использованием элементарных арифметических операций над элементами конечного поля и может быть выполнено алгоритмами полиномиальной сложности от параметров кода. Формально, асимптотическая емкостная сложность кодирования *(n, k, d)* кодами оценивается как *O(n)*, асимптотическая временная сложность оценивается как *O(kn)* и *O((n-k)n)* [22, 56].

2. Выработаны практические рекомендации по реализации предложенного метода декодирования алгеброгеометрических кодов на пространственных кривых. Разработаны алгоритмы и структурные схемы устройств алгебраического декодирования алгеброгеометрическими кодами на пространственных кривых. Показано, что сложность алгебраического декодирования предложенным методом растет полиномиально от исправляющей способности кода. Обоснована целесообразность реализации разработанных декодеров на современной вычислительной технике при исправляющей способности кода $t \leq 100$ [57, 58, 79].
3. Исследована помехоустойчивость передачи дискретных сообщений с использованием алгеброгеометрических кодов на пространственных кривых. Показано, что при фиксированной мощности алфавита символов и длине применение алгеброгеометрических кодов на пространственных кривых позволяет получить энергетический выигрыш от кодирования *0,5-0,8 dB* по сравнению с недвоичными кодами БЧХ [53].

Полученные результаты использованы в научно-исследовательских работах, проводимых в рамках Государственной научно-технической программы «Створення перспективних телекомунікаційних систем і технологій». Получены акты реализации результатов исследований при проведении научно-исследовательских работ и на производстве.

Достоверность полученных результатов обосновывается их непротиворечивостью основным положениям алгебраической теории кодов,

статистической теории связи и теории информации, а также сведением в некоторых упрощенных вариантах к известным результатам в теории помехоустойчивого кодирования.

Диссертационная работа состоит из введения, четырех разделов основной части, выводов по работе и приложений. Материал диссертации содержит 174 страницы, рисунков – 15, таблиц – 3. На отдельных листах 5 рисунков. Библиография из 130 наименований на 12 страницах. 2 приложения общим объемом 38 страниц.

В первом разделе анализируется структурная схема и математическая модель системы передачи дискретных сообщений, исследуются критерии и показатели качества их функционирования. Проводится анализ состояния, и исследуются пути развития методов помехоустойчивого кодирования, обосновывается выбор направления исследований и математически формализуется постановка научной задачи.

Во втором разделе разрабатывается метод помехоустойчивого кодирования алгеброгеометрическими кодами, заданными на пространственных кривых в P^3. Разрабатываются алгоритмы помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых и предложения по их аппаратной реализации.

В третьем разделе разрабатывается алгебраический метод декодирования алгеброгеометрических кодов на пространственных кривых. Разрабатываются алгоритмы и структурная схема устройства декодирования кодов на пространственных кривых. Исследуется сложность реализации декодеров алгеброгеометрических кодов на пространственных кривых.

В четвертом разделе исследуются математические модели каналов передачи данных и методики оценки помехоустойчивости. Проводится оценка помехоустойчивости передачи дискретных сообщений с использованием алгеброгеометрических кодов на пространственных кривых. Разрабатываются предложения по программной и аппаратной реализации

схем кодирования с использованием алгеброгеометрических кодов на пространственных кривых. Проводятся исследования помехоустойчивости передачи дискретных сообщений с использованием алгеброгеометрических кодов на пространственных кривых.

В выводах по работе сообщаются основные результаты проведенных исследований.

Основные результаты выполненной работы нашли свое отражение в 2-х отчетах о НИР и одном отчете о ОКР:

– в НИР «Розробка методів підвищення якості військового зв'язку автоматизованої системи управління ракетних військ і артилерії» шифр «Мрія», ГР № 0101U000414 разработаны алгоритмы алгеброгеометического кодирования и декодирования передаваемых кодограмм управления с использованием алгеброгеометрических кодов построенных на плоских алгебраических кривых, заданных в проективном пространстве P^2 неприводимым однородным уравнением от трех переменных [90];

– в НИР «Дослідженбня ефективних механізмів забезпечення конфіденційності, цілісності та доступності інформації» шифр «Облік», ГР № 0101U000668, разработаны криптосистемы на алгебраических блоковых кодах и построены теоретико-кодовые схемы на элептических кодах [26];

– в ОКР «Створення УКХ радіостанцій, що забезпечують енергетично скритний та перешкодозахищений радіозв'язок у повнозв'язаній мережі», которая проводилась в Центральном казенном конструкторском бюро "Протон", использованы метод и программная реализация помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых для повышения помехоустойчивости передачи дискретных сообщений, а также алгоритм декодирования алгеброгеометрических кодов на пространственных кривых.

Получено 3 акта о внедрении результатов диссертационной работы.

Публикации. Основные результаты исследований опубликованы в шести научных статьях [21, 22, 53, 55, 56, 79], и четырех тезисах докладов [57, 58, 59, 80].

Личный вклад автора диссертационной работы в публикации, выполненные в соавторстве, заключается в следующем:

- в [55] автором получены аналитические выражения для проведения декодирования алгеброгеометрических кодов по кривым в P^3, которые позволяют свести задачу декодирования к решению систем линейных уравнений, у которых число неизвестных задается конструктивными кодовыми характеристиками. Показано, что сложность алгебраического декодирования предложенным методом растет полиномиально от исправляющей способности кода;
- в [21] автором проведен анализ математической модели и структурной схемы систем передачи данных в телекоммуникационных системах и сетях;
- в [56] автором исследуется общая конструкция алгеброгеометрических кодов, как линейных систем, возникающих на проективных алгебраических кривых. Разработаны метод и алгоритмы помехоустойчивого кодирования алгеброгеометрическими кодами, заданными на пространственных кривых;
- в [22] автором разработаны практические алгоритмы кодирования алгеброгеометрическими кодами на пространственных кривых в систематическом и несистематическом виде. Оценена сложность их реализации;
- в [53] автором проводятся исследования помехоустойчивости передачи дискретных сообщений в телекоммуникационных системах с использованием алгеброгеометрических кодов на пространственных кривых в каналах с независимым распределением ошибок. Показано, что асимптотические свойства алгеброгеометрических кодов при увеличении длины кода и мощности алфавита символов обуславливают приближение к Шенноновской границе вероятности ошибочного приема символов

сообщения, что позволяет сделать вывод о высокой практической значимости полученных конструкций для повышения помехоустойчивости передачи дискретных сообщений в каналах с независимым распределением ошибок.

Основные результаты исследований докладывались и были одобрены на четырех научно-технических конференциях [57, 58, 59, 80]:

– Міжнародна науково-технічна конференція „Інтегровані комп'ютерні технології в машинобудуванні" ІКТМ-2006 (Харків, 2006) [57];

– Третья международная научная конференция „Современные методы кодирования в электронных системах" СМКЭС-2006 (Суми, 2006) [58];

– Перша науково-технічна конференція «Науково-методичні основи оцінювання та управління техногенною безпекою у разі виникнення надзвичайної ситуації». " (Харків, 2007) [59];

– Третя наукова конференція Харківського університету Повітряних Сил ім. Івана Кожедуба (Харків, 2007) [80].

В заключение автор выражает искреннюю благодарность научному руководителю кандидату технических наук, старшему научному сотруднику Кузнецову Александру Александровичу за оказанную помощь и поддержку при проведении исследований. Автор благодарен коллективу кафедры транспортного зв'язку Української Державної академії залізничного транспорту за ряд полезных советов и пожеланий, высказанных при обсуждении результатов диссертационной работы и оказанную помощь в ее оформлении.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Береза А.С. Основы построения АСУ. Основы структурного анализа и синтеза АСУ. – Х.: ХВУ, 1997. – 210 с.
2. Береза А.*С.* Основы построения АСУ. Системотехнические основы построения АСУ. – Х.: ХВУ, 1996. – 355 с.
3. Береза А.М. Основи створення інформаційних систем. – К., - 2001.– 214 с.
4. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир. - 1986. – 576с.
5. Блох Э.Л., Попов О.В., Турин В.Я. Модели источника ошибок в каналах передачи цифровой информации. – М.:Связью - 1971. – 312с.
6. Бондарев В.Н., Трестер Г. Цифровая обработка сигналов. – Х., 2001.- 400 с.
7. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник - СПб.: ИД Питер, 2002. - 688 с.
8. Бэрлэкэмп Э. Алгебраическая теория кодирования. Пер. с англ. Под ред. С.Д. Бермана. – М.:Мир. – 1971. – 477с.
9. Вавилов Е.Н., Портной Г.П. Синтез схем электронных цифровых машин. - М.: Советское радио. – 1963. – 440с.
10. Вентцель Е.С. Теория вероятностей: Учеб. для вузов – М., 2001. – 576 с.
11. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения. – М.: Наука, 1988. – 480 с.
12. Витерби А.Д., Омура Дж.К. Принципы цифровой связи и кодирования: Пер. с англ./ Под ред. К.Ш. Зигангирова.– М.: Радио и связь, 1982. - 535 с.
13. Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые // Современные проблемы маттематики. – М.: ВИНИТИ, 1984. Т. 25. С. 209-257.

14. Влэдуц С. Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеометрические коды. Основные понятия. – М.: МЦИМО, 2003. – 504 с.
15. Габидулин Э.М., Афанасьев В.Б. Кодирование в радиоэлектронике. – М.: Радио и связь. - 1986. – 176с.
16. Галузинський Г.П. Перспективні технологічні засоби оброблення інформації: - К., 2002. – 280 с.
17. Гетманцев В.Д. Лінійна алгебра і лінійне програмування. – К.: Либідь, 2001. – 255 с.
18. Гмурман В.Е. Теория вероятностей и математическая статистика: Учеб. пособие для вузов — М., 2002. — 480 с.
19. Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. 1981. Т.259. № 6. С. 1289-1290.
20. Грифитс Ф., Харрис Дж. Принципы алгебраической геометрии. – М.: Мир. - 1982.
21. Грабчак В.И. Пасько И.В. Лахтин С.Є. Королев Р.В. Анализ математической модели и структурной схемы системы передачи данных// Системи обробки інформації: Збірник наукових праць. – Х.: ХУ ПС, 2007. – Вип. 4 (62). – С. 30 - 34.
22. Грабчак В.И., Пасько И.В., Королев Р.В., Кужель И.Е. Алгебраический метод помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых // Системи управління, навігації та зв'язку. - К.: ЦНДІ навігації та управління – 2007.- Вип.3.- С. 82-85.
23. Додд А.З. Мир телекоммуникаций. Обзор технологий и отрасли: Пер. с англ. - М., 2002. - 400 с.
24. Долгов В.И. Основы статестической теории приема дискретных сигналов. - Х.: ХВВКИУ РВ, 1989.- 448 с.
25. Донской В.И. Дискретная математика. – Симф., 2000. – 360 с.
26. Дослідження ефективних механізмів забезпечення конфіденційності, цілісності та доступності інформації: Звіт про НДР // ХУ ПС.– Х., 2007. – 101с.

27. ДСТУ В 3265 – 95. Зв'язок військовий. Терміни та визначення. – К.: УкрНДІССІ, 1995. – 23 с.
28. Ж. Серр. Алгебраические группы и поля классов. – М.: Мир. - 1968.
29. Жураковський Ю.П., Полторак В.П. Теорія інформації та кодування. -К.: Вища школа, 2001.- 255 с.
30. Закон Украины «Про Концепцію Національної програми інформатизації» от 4 февраля 1998 г. N 75/98-ВР.
31. Згуровський М.З., Коваленко І.І. Вступ до комп'ютерних інформаційних технологій. – К., 2002. – 256 с.
32. Злотник Б. М. Помехоустойчивые коды в системах связи. – М.: Радио и связь. - 1989. – 232с.
33. Зюко А.Г., Кловский Д.Д. Теория передачи сигналов: - М.: Радио и связь, 1986. – 304 с.
34. Иванов М.Т., Сергиенко А.Б., Ушаков В.Н. Теоретические основы радиотехники: Учеб. пособие для вузов / – М., 2002. – 310 с.
35. Ильин В.А., Позняк Э.Г. Линейная алгебра. Учебн. для вузов. – 4-е издание. – М.: Наука. ФИЗМАТЛИТ. – 1999. – 296с.
36. Карпов Ю.Г. Теория автоматов. – СПб.: Питер, 2002. – 224 с.
37. Кацман Г. Л., Цфасман М. А. Спектры алгеброгеометрических кодов // Пробл. передачи информ. - Т. 23. № 4.- 1987. - С. 19 – 34.
38. Кларк Дж., мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи. – М.: Радио и связь. - 1987.
39. Коломієць В.Ф. Міжнародні інформаційні системи: Підруч. для ВНЗ - К., 2001. – 320 с.
40. Концепция Национальной программы информатизации одобренной Законом Украины «Про Концепцію Національної програми інформатизації» от 4 февраля 1998 г. № 75/98-ВР.

41. Коржик В.И., Финк Л.М. Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. – М.: – Связь, 1975 – 272 с.
42. Коррекция ошибок в оптических накопителях информации // Типикин А.П., Петров В.В., Бабанин А.Г.; Отв. Ред. Додонов А.Г.; АН УССР. Ин-т проблем регистрации информации. – Киев: Наук. Думка. - 1990. – 172с.
43. Котоусов А.С. Теория информации. – М.: Радио и связь, 2003. – 80 с.
44. Коуров Л.В. Информационные технологии: Учеб. пособие для студентов гуманитарных и экономических вузов – Мн., 2000. – 192 с.
45. Кремер Н.Ш. Теория вероятностей и математическая статистика. – М., 2000. – 543 с.
46. Кузьмин И.В., Кедрус В.А. Основы теории шифрования и кодирования: - К.: Вища школа, 1986.- 238 с.
47. Кузнецов А.А. Алгеброгеометрические коды // Электроника и системы управления. - К.: НАУ.- 2005-№ 2(4).-С.25-34.
48. Кузнецов А.А. Методика оценки энергетической эффективности двоичных блоковых кодов в каналах с группирующимися ошибками // Моделювання та інформаційні технології. - К.: НАНУ.- 2005- № 32. - С.116-124.
49. Кузнецов А.А. Методика оценки эффективности помехоустойчивого кодирования в каналах с группирующимися ошибками // Электронное моделирование: Международный научно-теоретический журнал. – К.: НАНУ, РАН, 2006. – №3. – С. 49-60.
50. Кузнецов А.А. Линейные блоковые коды на алгебраических кривых // Інформаційно-керуючі системи на залізничному транспорті. - Х.: ХарДАЗТ. - 2005 - № 1-2. - С.52-58.

51. Кузнецов А.А. Энергетическая эффективность алгеброгеометрических кодов // Электронное моделирование: Международный научно-технический журнал.- К.: НАНУ, РАН.- 2004 - № 2.- С.27-38.
52. Кузнецов А.А. Энергетический выигрыш алгеброгеометрического кодирования // Всеукр. меж вед. науч.-техн. сб. – Х.: ХТУРЭ, 2003. – Вып.134. – С. 218-222.
53. Кузнецов А.А., Грабчак В.И., Пасько И.В. Исследование помехоустойчивости передачи дискретных сообщений с использованием алгеброгеометрических кодов на пространственных кривых // Системи обробки інформації: Збірник наукових праць. –Х.: ХУПС, 2007. – Вип. 8 (66). – С. 134 - 138.
54. Кузнецов А.А., Евсеев С.П., Кужель И.Е., Грабчак В.И. Криптоанализ секретных систем, построенных с использованием алгебраических блоковых кодов // Системи обробки інформації: Збірник наукових праць. – Х.: ХУ ПС, 2005. – Вип. 8 (48). – С. 209-216.
55. Кузнецов О.О., Пасько І.В. Алгебраїчний метод декодування лінійних блокових кодів на алгебраїчних кривих у P^3 // Системи озброєння і військова техніка: науковий журнал. – 2006. – № 3 (7). – С. 69 - 72.
56. Кузнецов О.О., Пасько И.В., Королев Р.В. Алгебраический метод помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых // Системи обробки інформації: Збірник наукових праць. –Х.: ХУПС, 2007. – Вип. 5 (63). – С. 137 - 141.
57. *Кузнецов А.А., Пасько И.В.* Алгоритм алгебраического декодирования линейных блоковых кодов на пространственных кривых // Тези доповідей Міжн. НТК “Інтегровані комп’ютерні технології в машинобудуванні” (ІКТМ-2006). – Х.: Нац. аерокосм. ун-т “ХАІ ”, 2006. – С. 347.
58. Кузнецов А.А., Пасько И.В. Алгебраический метод декодирования линейных блоковых кодов на алгебраических кривых в P^3 // Тезисы докладов третьей международной научной конференции „Современные

методы кодирования в электронных системах" СМКЭС-2006, 24-25 октября 2006 года. – Сумы: СумДУ, 2006. – С. 10-11.

59. Кузнецов А.А., Пасько И.В. Алгеброгеометрические коды на пространственных кривых // Матеріали першої науково-технічної конференції «Науково-методичні основи оцінювання та управління техногенною безпекою у разі виникнення надзвичайної ситуації».– Х.: НДІ мікрографії.– 2007 – С. 8-9.
60. Кузнецов А.А., Северинов А.В., Задворный Д.А. Лысенко В.Н. Алгебраическое декодирование кодов по кривым Эрмита // Вестник ХПИ. – Харьков: НТУ "ХПІ" – 2003. – С 95-102.
61. Кузнецов А.А., Северинов А.В., Лысенко В.Н. Алгоритм мажоритарного декодирования алгеброгеометрических кодов // Системи обробки інформації. Збірник наукових праць. Вип. 4(26). – Харків: НАНУ, ПАНМ, ХВУ. - 2003. – С – 13-18.
62. Кузнецов А.А., Северинов А.В., Лысенко В.Н., Науменко И.В. Алгоритм помехоустойчивого кодирования с использованием кодов по кривым Эрмита // Системи обробки інформації. Збірник наукових праць. Вип. 6(28). – Харків: НАНУ, ПАНМ, ХВУ. - 2003. – С – 181-185.
63. Кузнецов А.А., Северинов А.В., Ивашкин А.В., Лысенко В.Н. Алгоритм декодирования алгеброгеоеметрических кодов. // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я. Анотації доповідей міжнародної науково-практичної конференції 15-16 травня 2003 р. – Харків: НТУ "ХПІ". – 2003. – С. 26.
64. **Кузнецов А. А., Ушно С. В. Поиск неприводимых алгебраических кривых малой степени в конечных полях. //Системи обробки інформації. – Харків: НАНУ, ПАНИ, ХВУ. – 2000. – С 147-150.**
65. Кулаков Ю.О. Комп'ютерні мережі: Підруч. для ВНЗ — К., 2002. — 432 с.

66. Кэйнал Л.Н., Састри А.Р.К. Модели каналов с памятью и их применение для защиты от ошибок / Тр. ин-та инженеров по электротехн. и радиоэлектр. – 1978. –66, №7. – С.5-29.
67. Лидл Р., Нидеррайтер Г. Конечные поля: Пер. с англ.: В 2т. – М.: Мир, 1988. – Т. 1. – 430 с.
68. Лидл Р., Нидеррайтер Г. Конечные поля: Пер. с англ.: В 2т. – М.: Мир, 1988. – Т. 2. – 392 с. Ломовицкий В.В. Основи построения систем и сетей передачи информации. Учебное пособие для вузов. – М.: ГЛТ, 2005. – 382 с.
69. Лосев В.В., Бродская Е.Б. Поиск и декодирование сложных дискретних сигналов: - М.: Радио и связь, 1988. – 224 с.
70. Мелихов А.Н. Ориентированные графы и конечные автоматы. – М.: Наука. – 1971. – 416с.
71. Мутер В.М. Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат. Ленингр. Отд-ние. - 1990. – 288с.
72. Надежность и эффективность в технике: Справочник. В 10 т./Ред. совет: В.С. Авдуевский и др.– М.: Машиностроение, 1988. - Т.3.- 328 с.
73. Надежность и эффективность в технике: Справочник: В 10 т./ Ред. совет: В.С. Авдуевский и др. – М.: Машиностроение, 1986. – Т.1. – 224с.
74. Науменко М.І., Стасєв Ю.В., Кузнецов О.О. Алгеброгеометричне узагальнення лінійних блокових кодів // Системи озброєння і військова техніка. – Х.: ХУ ПС, 2005. – Вип. 2 (2). – С. 15-31.
75. Науменко М.І., Стасєв Ю.В., Кузнєцов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів. Монографія - Х.: ХУ ПС, 2005. - 267 с.
76. Нефедов В.И. Основы радиоэлектроники и связи: Учеб. для вузов – М., 2002. – 510 с.
77. Олифер В.Г. Компьютерные сети. – СПб.: ИД Питер, 2002. – 864 с.

78. Основы компьютерных технологий: Учеб. пособие / Попов В.Б. – М., 2002. – 704 с.
79. Пасько И.В. Алгебраическое декодирование кодов на пространственных кривых // Системи обробки інформації: Збірник наукових праць.– Х.: ХУПС, 2007. – Вип. 1 (59). – С. 121 - 125.
80. Пасько И.В. Алгебраическое декодирование кодов на пространственных кривых // Матеріали третьої наукової конференції Харківського університету Повітряних Сил ім. Івана Кожедуба. – Х.: ХУ ПС. – 2007. – С. 96-97.
81. Петров М. Информационные системы: Учеб. для вузов – СПб.: ИД Питер, 2001. – 688 с.
82. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир. - 1976. – 596 с.
83. Полознюк О.Е. Конспект лекций по высшей математике. – Ч. 1: Линейная алгебра. Векторная алгебра. Аналитическая геометрия. – К., 2002. – 104 с.
84. Помехоустойчивость и эффективность систем передачи информации. А.Г. Зюко, А.И. Фалько, И.П. Панфилов, В.Л. Банкет, П.В. Иващенко; Под. Ред. А.Г. Зюко. – М.: Радио и связь. - 1985. – 272с.
85. Помехоустойчивое кодирование и надежность ЭВМ: - М.: Наука, 1987. – 191 с.
86. Пономаренко В.С. Проектування інформаційних систем: Навч. посіб. для ВНЗ. – К.:ВЦ Академія, 2002. – 496 с.
87. Постановление Кабинета Министров Украины «Про Концепцію розвитку зв'язку України до 2010 року» от 9 декабря 1999 г. №2238.
88. Прокис Дж. Цифровая связь. – М.: Радио и связь. – 2000. – 800с.
89. Пятибратов А.П. Вычислительные системы, сети и телекоммуникации.– М., 2003. – 512 с.

90. Розробка методів підвищення якості військового зв’язку автоматизованої системи управління ракетних військ і артилерії: Звіт про НДР // ХУ ПС. – Х., 2006. – 133 с.
91. Руководство по технологиям объединенных сетей / Cisco Systems. - М.: Вильямс, 2002. – 1040 с.
92. Савицкий Н.И. Технологии организации, хранения и обработки данных. – М., 2001. – 232 с.
93. Северинов А.В., Кузнецов А.А., Куриш В.В. Разработка алгоритма декодирования алгеброгеометрических кодов // Системи обробки інформації. – Харків: НАНУ, ПАНИ, ХВУ.– №1(17). – 2002. – С. 161-163.
94. Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение. Изд.2-е, испр.: Пер. с англ.- М.: Издательский дом «Вильямс», 2004. - 1104с.
95. Стеклов В.К., Беркман Л.Н. Проектування телекомунікаційних мереж: Підруч. для ВНЗ. - К.: Техніка, 2002. - 792 с.
96. Стєклов В.К. Основи управління мережами та послугами телекомунікацій: Підруч. для ВНЗ – К.: Техніка, 2002. – 440 с.
97. Столлингс В. Компьютерные системы передачи данных. – М.: Вильямс, 2002. – 928 с.
98. Судоплатов С.В., Овчинникова Е.В. Элементы дискретной математики. – М., 2002. – 280 с.
99. Теория кодирования: Пер. с япон./ Т. Касами, Н. Токура, Е. Ивадари, Я. Инагаки /Под ред. Б.С. Цыбакова и С.И. Гельфанда.– М.: Мир, 1978.– 576с.
100. Уолрэнд Дж. Телекоммуникационные и компьютерные сети. – М.: Постмаркет, 2001. – 480 с.
101. Фигурин В.А., Оболонин В.В. Теория вероятностей и математическая статистика. – Мн., 2000. – 208 с.

102. Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн. Теория кодов, исправляющих ошибки.- М.: Связь. - 1979. - 744 с.
103. Хартли Р. Передача информации. // Теория информации и ее приложения. Сборник переводов.– М.: ФИЗМАТГИЗ.– 1959.– С.5-35.
104. Хопкрофт Джон. Введение в теорию автоматов, языков и вычислений. – М.: Вильямс, 2002. – 528 с.
105. Цфасман М.А. Коды Гоппы, лежащие выше границы Варшамова - Гилберта. //Проблемы передачи информации. – Москва. - №3 –1982. - С. 3-6.
106. Цымбал В.П. Теория информации и кодирование:-К.: Вища школа, 1992.- 262 с.
107. Шафаревич И.Р. Основы алгебраической геометрии. – М.: Наука. - 1972.
108. Шеннон К. Работы по теории информации и кибернетике. –М.: ИЛ. – 1963. – 829с.
109. Шеннон К. Связь при наличии шума. // Теория информации и ее приложения. Сборник переводов.– М.: ФИЗМАТГИЗ.- 1959. - С.82-112.
110. Шиллер Й. Мобильные коммуникации — М.: Вильямс, 2002. — 384 с.
111. Шрюфер Е. Обробка сигналів: цифрова обробка сигналів. Підручник // за ред.. В.П. Байка: - К.: Либідь, 2000. - 296 с.
112. Элементы теории передачи дискретной информации. Л.П. Пуртов, А.С. Замрий, А.И. Захаров, В.М. Охорзин; Под ред. Л.П. Пуртова. – М.: – Связь, 1972 – 232 с.
113. Яблонский С.В. Введение в дискретную математику.– М., 2002. – 384 с.
114. B.-Z. Shen, G.J.M. van Wee, Ruud Pellikaan; Which linear codes are algebraic-geometric ?, IEEE Trans. Inform. Theory. IT-37 (1991), 583-602.
115. Berlekemp E.R. Algebraic coding theory.- New York: McGraw-Hill, 2003
116. C. Munuera, Ruud Pellikaan; Equality of geometric Goppa codes and equivalence of divisors, Journ. Pure Appl. Algebra 90 (1993), 229-252.

117. C. Munuera, Ruud Pellikaan; Self-dual and decomposable geometric Goppa codes, in Eurocode 92, (P.Camion, P. Charpin and S. Harari eds.), Udine, CISM Courses and Lectures 339, Springer-Verlag, Wien-New York, 2000, 77-87

118. Farrán, J.I.; Lossen, C.: `brnoeth.lib`. A SINGULAR 2.0 library for computing AG codes and Weierstraß semigroups (2001).

119. Feng G.L., Rao T.R.N. Decoding algebraic geometric codes up to the designed minimum distance // IEEE Trans. Inform. Theory. – 1993. – Vol. 39, N 1 – P. 37-46.

120. Greuel, G.-M.: Computer Algebra and Algebraic Geometry - Achievements and Perspectives. J. Symbolic Computation 30,3, 253-290 (2000).

121. Ian Blake, Chris Heegard, Tom Hoholdt, Victor K. W. Wei; Algebraic-Geometry Codes, IEEE Trans. Info. Theory, vol. IT-44, pp. 2596 - 2618, October 1998.

122. Johan P. Hansen; Codes on the Klein quartic, ideals, and decoding (Corresp.), IEEE Trans. Info. Theory, vol. IT-33, pp. 923 - 925, November 1987.

123. Ruud Pellikaan, H. Stichtenoth, F. Torres; Weierstrass semigroups in an asymptotically good tower of function fields, Finite Fields and their Applications, vol. 4, pp. 381-392, 1998.

124. Ruud Pellikaan; Asymptotically good sequences of curves and codes, in Proc. 34th Allerton Conf. on Communication, Control, and Computing, Urbana-Champaign, October 2-4, 1996, 276-285.

125. Ruud Pellikaan; On special divisors and the two variable zeta function of algebraic curves over finite fields, in Arithmetic, Geometry and Coding Theory 4, Luminy 1993, (R. Pellikaan, M. Perret and S.G. Vladut eds.), Walter de Gruyter & Co, Berlin 1996, 175-184.

126. Ruud Pellikaan; The Klein quartic, the Fano plane and curves representing designs, in Codes, Curves, and Signals: Common Threads in Communications, (A. Vardy, Ed.), pp. 9-20, Kluwer Acad. Publ., Dordrecht 1998.

127. Ruud Pellikaan; The shift bound for cyclic, Reed-Muller and geometric Goppa codes, in Arithmetic, Geometry and Coding Theory 4, Luminy 1993, (R. Pellikaan, M. Perret and S.G. Vladut eds.), Walter de Gruyter & Co, Berlin 1996, 155-174.

128. Sakata S., Justesen J., Madelung Y., Jensen H.E., Hoholdt T. Fast Decoding of Algebraic-Geometric Codes up to the Designed Minimum Distance // IEEE Trans. Inform. Theory. – 1995. – Vol. 41, N 5 – P. 1672-1677.

129. T. Hoholdt, J.H. van Lint, Ruud Pellikaan; Algebraic geometry codes, in Handbook of Coding Theory, vol 1, pp. 871-961, (V.S. Pless, W.C. Huffman and R.A. Brualdi, Eds.) Elsevier, Amsterdam 1998.

130. Voss, Tom Hoholdt; An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound. The first steps, IEEE Trans. Info. Theory, vol. IT-43, pp. 128 - 135, January 1997.