На правах рукописи

АЛЕКСЕЕВ Максим Олегович

Методы нелинейного кодирования для повышения достоверности обработки информации

Специальность 05.13.01– Системный анализ, управление и обработка информации (технические системы)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург − 2015

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (ГУАП).

Научный руководитель: **Мирончиков Евгений Тимофеевич**,

доктор технических наук, профессор, Санкт-Петербургский государственный университет аэрокосмического приборостроения, профессор кафедры «Аэрокосмические компьютерные и программные системы»

Официальные оппоненты: **Яковлев Виктор Алексеевич**,

доктор технических наук, профессор, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, профессор кафедры «Защищённые системы связи»

Трифонов Пётр Владимирович,

кандидат технических наук, доцент, Санкт-Петербургский государственный политехнический университет, доцент кафедры «Распределенные вычисления и компьютерные сети»

Ведущая организация – Санкт-Петербургский филиал "Научно-исследовательского и проектно-конструкторского института информатизации, автоматизации и связи на железнодорожном транспорте" (СПбФ ОАО «НИИАС»), г. Санкт-Петербург.

Защита состоится «29» сентября 2015 г. в 13:00 на заседании диссертационного совета Д 002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук по адресу: 199178, Санкт-Петербург, В.О.,14 линия, 39.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.

http://www.spiiras.nw.ru/dissovet/

Автореферат разослан «____» _____ 2015 г.

Учёный секретарь
диссертационного совета Д 002.199.01,
кандидат технических наук Р. Р. Фаткиева

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Исследование и разработка методов помехоустойчивого кодирования, обеспечивающих достоверность и целостность информации в автоматизированных системах обработки информации и управления, в системах и сетях передачи данных на протяжении многих лет остается актуальной задачей. Это объясняется, с одной стороны, постоянно возрастающими объемами информации, обрабатываемой и хранимой в таких системах, а с другой – значительно возросшими требованиями к достоверности информации, передаваемой по каналам с шумами.

Принципиальная возможность обеспечения сколь угодно высокой достоверности передачи (хранения) информации для широкого класса каналов связи с отличной от нуля пропускной способностью была доказана К. Шенноном в его фундаментальной работе «Теория информации. Математическая теория связи», опубликованной в 1948 году. Поиск конструктивного доказательства теоремы К. Шеннона стимулировал многочисленные исследования, которые сформировали современную теорию помехоустойчивого кодирования. Основной задачей этой теории является построение кодов с характеристиками, обещанными теоремой К. Шеннона, которые имели бы конструктивные методы кодирования и декодирования.

Эффективность использования помехоустойчивого кода для обнаружения/исправления ошибок в канале передачи (хранения) информации зависит от того, насколько корректирующие свойства кода согласованы с закон распределения шума в канале. В алгебраической теории помехоустойчивого кодирования, занимающейся блоковыми кодами, задачу согласования шума канала с корректирующей способностью кода принято описывать в терминах метрики пространства ошибок, согласованной с кодом.

Если удаётся найти метрику, согласованную с шумами канала, то задача построения наилучшего блокового кода сводится к поиску некоторого подмножества пространства, обладающего заданными метрическими свойствами. Это подмножество и является помехоустойчивым кодом, способным обнаруживать/корректировать наиболее вероятные ошибки канала

Известно, что подавляющее большинство результатов теории помехоустойчивого кодирования относится к кодам, обнаруживающим/исправляющим ошибки в каналах, согласованных с метрикой Хэмминга, то есть каналах, описываемых моделью q-ичного симметричного канала без памяти или, другими словами, дискретным отображением канала с белым гауссовским шумом. Однако, как показывают многочисленные экспериментальные исследования, реальные каналы передачи и хранения информации таковыми каналами не являются. Л.М. Финк и В.И. Коржик назвали эти каналы каналами со случайной структурой. Попытки найти метрику, согласованную с шумами для сколь-нибудь широкого класса таких каналов, не привели к успеху.

Существуют два подхода к решению вопроса обеспечения помехоустойчивости и целостности информации при передаче (хранении) в таких каналах.

Первый связан с поиском специальных преобразований на входе и выходе канала, позволяющих обеспечить согласование преобразованного шума канала с корректирующими свойствами кода, исправляющего ошибки в метрике Хэмминга. Простейшим примером такого преобразования может служить декорреляция. Более сложные преобразования были предложены в работах Е. Элайеса, Д. Форни, Е.Т. Мирончикова, Г.Ш. Полтырева и Н.А. Шехуновой.

Другой подход предполагает построение специальных методов преобразования данных – кодов, позволяющих обнаруживать (исправлять) любые комбинации ошибок с некоторой отличной от нуля вероятностью. Первым шагом к построению таких методов, по-видимому, следует считать нелинейный код Васильева. Коды, предложенные в разное время в работах Фелпса, Моллера, Карповского, а также учеников Васильева Соловьевой, Августиновича и др. значительно развили этот подход.

Следует заметить, что авторы этих работ в качестве математической модели канала часто используют канал с алгебраическими манипуляциями. Как правило, модель алгебраической манипуляции понимается как изменение содержимого некоторого абстрактного запоминающего устройства на заданную величину при условии отсутствия зависимости между внутренним состоянием устройства и привносимой ошибкой. В модели рассматривается аддитивная ошибка, значение которой может принимать любое ненулевое значение из некоторого конечного алфавита. Таким образом, каналом с алгебраическими манипуляциями является канал, для которого характерно возникновение произвольных ошибок.

Диссертация посвящена разработке и исследованию кодовых методов, позволяющих организовать достоверную передачу, хранение и обработку данных в канале с алгебраическими манипуляциями, обеспечивая их целостность. Под целостностью данных часто понимают то условие, что данные полны и не были изменены при их обработке (передаче, хранении, представлении). Получаемые коды гарантируют заданный уровень обнаружения любых искажений вне зависимости от их природы и источника. Таким образом, основным содержанием диссертации являются теоретические и прикладные исследования методов обработки информации, позволяющие повысить надёжность и качество функционирования систем передачи, хранения и обработки информации. Кодовые методы повышения помехозащищённости основываются на теории помехоустойчивого кодирования, однако используют ранее не исследовавшиеся классы нелинейных кодов, обнаруживающих алгебраические манипуляции.

Цель работы состоит в разработке и исследовании новых кодовых методов и алгоритмов декодирования, повышающих достоверность обработки информации, подвергающейся алгебраическим манипуляциям, и обладающих меньшей вычислительной сложностью по сравнению с известными. Использование этих кодов в системах передачи, хранения и обработки информации позволит повысить надежность обработки и помехозащищённость информации в каналах, описываемых моделью ал-

гебраических манипуляций. Таким образом, решается актуальная проблема разработки современных методов и алгоритмов решения задач обработки информации.

В соответствии с целью работы были поставлены следующие **задачи диссертационного исследования**:

1) Разработка и исследование кодового метода повышения помехоустойчивости на основе класса обобщённых систематических надёжных кодов, обнаруживающих алгебраические манипуляции.

2) Разработка алгоритма обнаружения и исправления ошибок малой кратности с помощью обобщённых систематических надёжных кодов.

3) Разработка и исследование кодового метода повышения помехоустойчивости, основанного на операции скалярного умножения компонентов информационного сообщения и значения случайной величины.

4) Модификация известного кодового метода повышения помехоустойчивости, основанного на операции умножения информационного и случайного компонентов, с целью уменьшения информационной избыточности.

5) Теоретико-информационный анализ нелинейных кодов, позволяющий вывести оценки (построить границы) экстремальных значений их параметров.

Методы исследования. Для решения поставленных задач использовались методы теории информации, теории помехоустойчивого алгебраического кодирования, теории вероятностей и элементы теории нелинейных функций над конечными полями.

Степень достоверности результатов определяется корректным использованием математического аппарата указанных выше теорий, апробацией результатов работы, а также положительными итогами практического использования результатов диссертационной работы в ЗАО «Научные приборы» и в ГУАП. Результаты находятся в соответствии с результатами, полученными другими авторами.

Научной новизной обладают следующие результаты работы:

1) Кодовый метод повышения помехоустойчивости, основанный на классе обобщённых систематических надёжных кодов. Данные коды при определённых параметрах позволяют обнаруживать сильные манипуляции с большей вероятностью, чем существующие коды. Кроме того, преимуществом данных кодов является существование простых алгоритмов исправления ошибок и возможности использования схемы гибридного кодека.

2) Алгоритм обнаружения и исправления ошибок малой кратности для обобщённых систематических надёжных кодов. Данный алгоритм обладает меньшими информационной избыточностью и вычислительной сложностью, чем существующие альтернативы.

3) Кодовый метод повышения помехоустойчивости, основанный на операции скалярного умножения компонентов информационного сообщения и значения случайной величины. Получаемый код отличается от других кодов, основанных на операции

умножения в конечном поле, возможностью варьировать размер проверочной части кодового слова. Отличие от существующих кодов, обнаруживающих алгебраические манипуляции, заключается в большей вероятности обнаружения помех и меньшей вычислительной сложности.

4) Нижняя граница вероятности необнаружения алгебраической манипуляции, полученная для кодов, основанных на обобщённых кодах Рида–Маллера. Данная граница является уточнением существующей границы для кодов, обнаруживающих алгебраические манипуляции, применительно к конкретному методу построения кода.

5) Нижняя граница длины систематического равномерно надёжного кода, являющаяся улучшением нижней границы для надёжных кодов в систематическом представлении.

Практическая значимость диссертации заключается в том, что в ней разработаны математические методы обеспечения целостности и повышения помехозащищённости данных в каналах со случайной структурой, которые могут быть описаны моделью алгебраических манипуляций. Данные методы позволяют не только указать параметры кодов и построить алгоритмы их декодирования, но и дают возможность количественно оценить качество их использования на практике при обработке, передаче и хранении информации в каналах с алгебраическими манипуляциями.

Результаты диссертации используются для повышения надёжности при хранении информации в твердотельной памяти бортовых накопителей и при обработке её в вычислительных устройствах, устойчивых к привнесённым помехам. Кроме того, коды, получаемые с помощью предлагаемых методов построения, могут быть применены в смежных областях, включающих надёжные схемы разделения секрета, нечёткие экстракторы и другие.

Внедрение и реализация результатов работы. Основные результаты работы были использованы при выполнении научно-исследовательской работы по разработке и исследованию надёжных методов хранения информации в аэрокосмических системах и комплексах, выполняемой по заданию № 2.2716.2014/К Минобрнауки России. Код, основанный на операции скалярного умножения компонентов информационного сообщения и значения случайной величины, также был использован в ЗАО «Научные приборы» при разработке методов проектирования электронных идентификационных документов в рамках выполнения научно-исследовательской работы. Кроме того, теоретические результаты работы используются в учебном процессе кафедры аэрокосмических компьютерных и программных систем Санкт-Петербургского государственного университета аэрокосмического приборостроения.

Апробация работы. Основные результаты работы докладывались и обсуждались на следующих семинарах, конференциях и симпозиумах:

Научных сессиях ГУАП (Санкт–Петербург, Россия, 2011-2013, 2015); семинаре лаборатории «Reliable Computing Laboratory» Бостонского университета (Бостон, США, 2011); Всероссийской научной конференции по проблемам информатики «СПИСОК» (Санкт–Петербург, Россия, 2012); 23–ей научно–технической конферен-

ции «Методы и технические средства обеспечения безопасности информации» (Санкт–Петербург, Россия, 2014); семинаре «Информатика и компьютерные технологии» СПИИРАН (Санкт–Петербург, Россия, 2014), симпозиуме «Workshop on Coding and Cryptography» (Париж, Франция, 2015).

Публикации. Результаты, представленные в диссертационной работе, опубликованы в 12 печатных работах. Среди них 5 работ опубликованы в изданиях, включённых в перечень ВАК.

Основные положения, выносимые на защиту:

1) кодовый метод повышения помехоустойчивости на основе класса обобщённых систематических надёжных кодов, обнаруживающих алгебраические манипуляции;

2) алгоритм обнаружения и исправления ошибок малой кратности с помощью обобщённых систематических надёжных кодов;

3) кодовый метод повышения помехоустойчивости, основанный на операции скалярного умножения компонентов информационного сообщения и значения случайной величины, а также его модификации;

4) границы экстремальных значений параметров нелинейных кодов, обнаруживающих алгебраические манипуляции.

Объем и структура работы. Диссертационная работа состоит из введения, пяти глав, заключения, приложения, списка использованных источников (145 наименований), а также списков использованных сокращений. Диссертация содержит 115 страниц, включая 6 таблиц и 17 рисунков. Приложение содержит 35 страниц, включая 14 рисунков и 1 таблицу.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность выбранной темы, определена цель и сформулированы решаемые в работе задачи. Перечислены новые научные результаты, полученные при выполнении работы, показаны практическая значимость и апробация работы, описаны внедрение и реализация результатов. Приведены основные положения, выносимые на защиту.

В первой главе работы рассматривается модель канала с алгебраическими манипуляциями и приводятся её основные практические приложения.

Алгебраическая манипуляция, как правило, понимается как изменение содержимого некоторого абстрактного запоминающего устройства на заданную величину (ошибку) при условии отсутствия зависимости между внутренним состоянием устройства и величиной привносимого искажения. Привносимая ошибка является аддитивной и может принимать любое ненулевое значение. В работе приводится метод преобразования любого канала в канал с аддитивными ошибками, что позволяет применять модель алгебраических манипуляций к широкому кругу реальных каналов. Количественной мерой надёжности обработки информации в канале с алгебраи-

ческими манипуляциями выступает вероятность необнаружения манипуляций. Алгебраические манипуляции делятся на два вида: слабые и сильные.

Слабая модель манипуляций используется для описания ситуаций, когда отсутствует зависимость между привносимой ошибкой и данными, поступившими на вход устройства. Необходимо уточнить, что внутри устройства входные данные могут подвергаться некоторому преобразованию (например, помехоустойчивому кодированию или шифрованию), поэтому в общем случае, хранимые данные (состояние устройства) отличаются от поступивших на вход устройства. Другими словами, слабая манипуляция описывает ситуацию, когда значение привносимой ошибки случайно, не зависит от входных данных и зачастую принимается равномерно распределённой случайной величиной. Вероятность необнаружения слабых манипуляций будет обозначаться P^{w}_{undet}.

Модель сильных алгебраических манипуляций используется в тех случаях, когда между входными данными и привносимой ошибкой существует зависимость. Примером канала с сильными манипуляциями является асимметричный канал, в котором величина возникающей ошибки напрямую зависит от поступающих данных. При сильных манипуляциях может достигаться большая вероятность необнаруживаемого искажения информации, обозначаемая P^{s}_{undet}. В работе будет рассматриваться верхняя граница данной вероятности, что позволит гарантировать достоверность обработки информации во всех каналах с сильными манипуляциями без учета зависимости между ошибками и данными.

Если информация, поступающая в устройство, хранится в нём в исходном виде (то есть не используются методы кодирования), то при считывании информации пользователь не сможет установить факт её искажения. Очевидно, что такая ситуация является крайне нежелательной. Таким образом, актуальной является задача разработки такого преобразования входных данных внутри устройства, которое позволит обнаруживать факт искажения. Алгебраическую манипуляцию будем считать успешной, если при обработке данных привнесённая ошибка не была обнаружена. Следовательно, качество надёжности обработки и передачи информации определяется вероятностью необнаружения манипуляции или, что в данном случае одно и тоже, вероятностью необнаружения привнесённого искажения.

Задача обнаружения алгебраических манипуляций была сформулирована в 2008 году для схем разделения секрета, среди участников которых присутствуют мошенники. Воздействие ионизирующего космического излучения (солнечная радиация, галактическое космическое излучение, радиационные пояса Земли и так далее) на аэрокосмическое оборудование также может рассматриваться как канал с алгебраическими манипуляциями. Другой областью применения данной модели канала является привнесение помех в работу устройства.

Во второй главе рассматриваются основные методы защиты вычислительных устройств от помех. Как уже было отмечено, успешное обнаружение привнесённых

помех гарантирует обеспечение целостности данных в канале с алгебраическими манипуляциями. Классическим подходом для проектирования устройств, устойчивых к помехам, является использование техники параллельного обнаружения ошибок. Общая схема параллельного обнаружения ошибок приведена на рисунке 1. Примеры характеристик $g(i)$: само значение $g(i)$ (дублирование), чётность $g(i)$, количество нулевых или единичных битов в $g(i)$ и так далее.

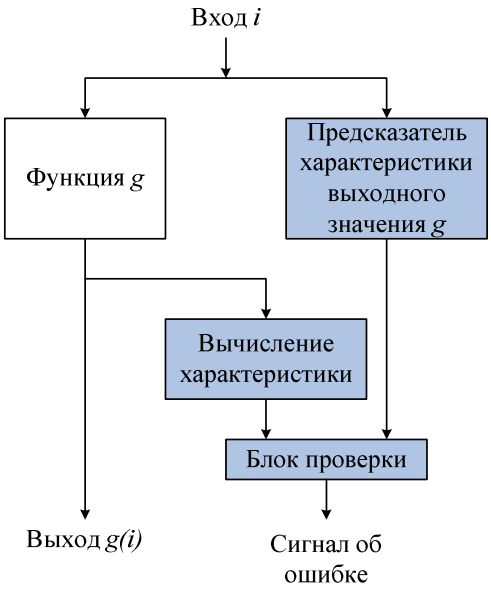

Рисунок 1 – Общая схема параллельного обнаружения ошибки

Любая схема, предназначенная для борьбы с помехами, характеризуется набором или классом ошибок, при наличии которых нарушается целостность данных, то есть происходит их необнаруживаемое искажение. Под обеспечением целостности данных понимается такое поведение системы, при котором система либо выдаёт корректные выходные данные, либо сигнализирует о выдаче ошибочных данных. Основную угрозу для целостности данных представляют необнаруживаемые ошибки. Для заданного метода защиты будем считать необнаруживаемой такую ошибку, возникновение которой не может быть обнаружено с помощью этого метода. Другими словами, ошибка e является необнаруживаемой в том случае, если для любой разрешённой обрабатываемой комбинации $v \in V$ выполняется равенство $e + v = u \in V$, где V есть множество разрешённых обрабатываемых комбинаций. Множество необнаруживаемых ошибок, внедрение которых будет успешным при любых обрабатываемых данных, будем называть постоянной конфигурацией необнаруживаемых ошибок.

В данной главе рассматриваются следующие методы обеспечения помехозащищённости:

- дублирование оборудования;
- использование линейных помехоустойчивых кодов;
- хеширование;
- использование нелинейных помехоустойчивых кодов.

Дублирование оборудования является наиболее очевидным методом борьбы с искажениями. При защите вычислительного блока создается его копия, которая используется наравне с оригинальным устройством. Выходные данные обоих блоков сравниваются, и при наличии различий между ними принимается решение об искажениях данных. Схема параллельного обнаружения ошибок с помощью дублирования оборудования приведена на рисунке 2.

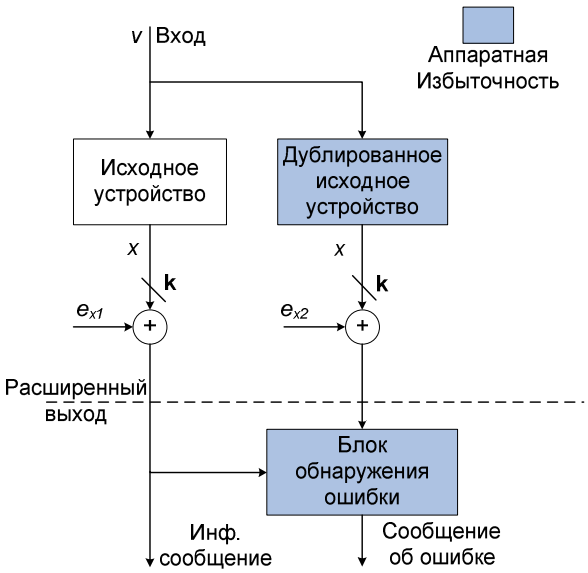

Рисунок 2. Схема обнаружения ошибок с использованием дублирования оборудования

При рассмотрении данного метода защиты с точки зрения описанных моделей алгебраических манипуляций видно, что возникновение одинаковых конфигураций ошибок в оригинальном и дублирующем блоках приводит к необнаруживаемым ошибкам. Таким образом, дублирование оборудования не обеспечивает защиту устройств от рассматриваемых моделей ошибок.

Другим классическим методом защиты от помех является использование линейных помехоустойчивых кодов. Наибольшее распространение получили систематические коды, что объясняется уменьшенной задержкой обработки и простотой их встраивания в схемы параллельного обнаружения ошибок. В качестве характеристики, которую вычисляет предсказатель, используется значение проверочных символов линейного кода. Пример использования линейных кодов в схемах параллельного обнаружения ошибки приведён на рисунке 3.

Несмотря на то, что кодер и предсказатель изображены как отдельные блоки, формально, предсказателем является их совокупность. Но для более наглядной демонстрации использования помехоустойчивых кодов в схемах параллельного обнаружения ошибок на рисунке кодер был выделен в отдельный блок. При таком делении предсказатель сводится к блоку, осуществляющему преобразование аналогично исходному устройству, но, возможно, над данными другой размерности (если $k \neq r$).

Кодер вычисляет функцию (характеристику) от этого значения. За счёт линейности преобразований возможен любой порядок расположения блоков предсказания и кодирования.

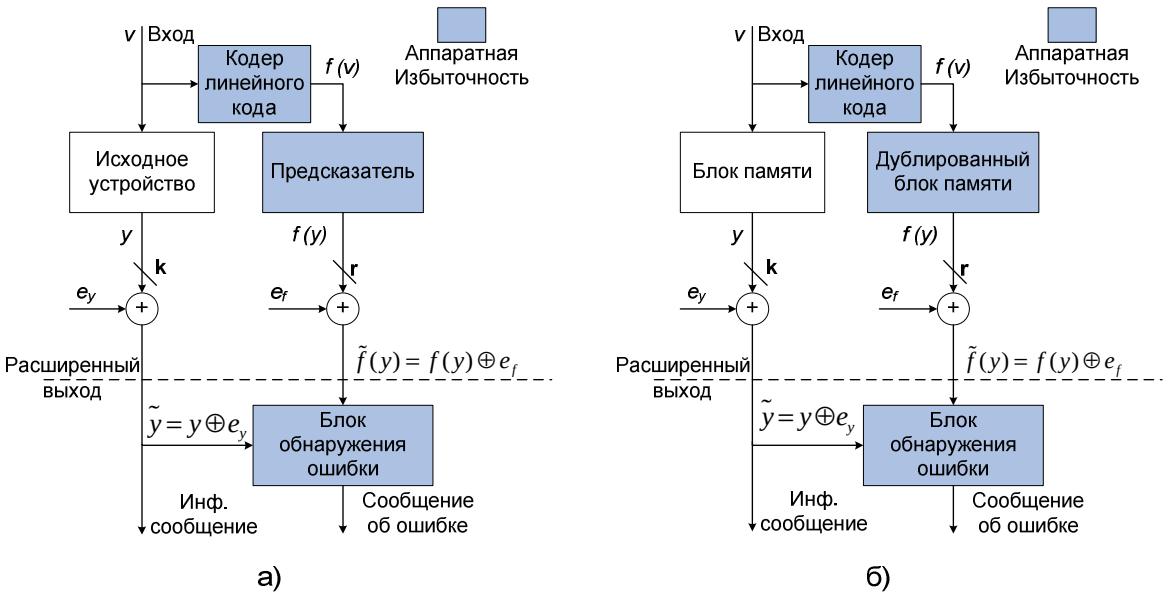

Рисунок 3. Пример схемы параллельного обнаружения ошибок с использованием линейных помехоустойчивых кодов: а) для защиты линейных блоков вычислительных устройств; б) для защиты блоков памяти

Любой q-ичный линейный код размерности k в силу своей линейности имеет $q^k - 1$ необнаруживаемых ошибок, соответствующих кодовым словам. Следовательно, даже при слабой модели алгебраических манипуляций возникновение искажений (ошибок), соответствующих кодовым словам, будет приводить к необнаружению манипуляций линейным кодом. Стоит отметить, что дублирование оборудования можно рассматривать как использование линейного кода−повторения.

Хеширование является другим классическим методом обеспечения целостности данных. Принцип использования хеш-функций аналогичен применению помехоустойчивого кодирования и заключается в вычислении информационной избыточности, называемой хешем или сводкой сообщения. Повторное вычисление хеша после передачи данных по каналу (обработки) и сравнение его с исходным значением хеша позволяет проверять целостность переданных (обработанных) данных.

Легко заметить, что относительно простые хеш−функции на основе контрольных сумм, зачастую являющиеся частным случаем использования ЛПК (например, хеш на основе CRC), не обеспечивают защиту от искажений, описываемых моделью алгебраических манипуляций. Стойкие хеш−функции позволяют обеспечить обеспечение целостности при алгебраических манипуляциях (в случае сильных манипуляций − при использовании криптографической соли (строки случайных данных)). Однако, фиксированный размер хешей и их относительно высокая вычислительная сложность накладывают значительные ограничения на их применимость в технических системах. Требования, предъявляемые к стойким хеш−функциям, значительно

превышают требования к методам защиты от алгебраических манипуляций, поэтому имеет смысл использовать более простые методы, о которых будет сказано далее.

Естественным решением проблемы линейных кодов и хеширования стало использование нелинейных кодов. Среди нелинейных кодов существуют классы кодов, которые обеспечивают обнаружение любой ошибки с заданной ненулевой вероятностью. Согласно данному ранее определению необнаруживаемых ошибок, данные классы кодов их не имеют. Другими словами, множество конфигураций ошибок, возникновение которых будет необнаруживаемым при любых обрабатываемых данных, является пустым. Таким образом, вне зависимости от значения искажения, данные классы кодов гарантируют её обнаружение с заданной вероятностью.

Далее будут рассматриваться коды над конечными полями характеристики два, однако большинство результатов может быть обобщено для любых полей.

Вычисление проверочных символов нелинейных кодов осуществляется с помощью нелинейных функций. Пусть f есть функция, отображающая элементы поля $GF(2^k)$ в поле $GF(2^r)$: $f(a)=b$. Нелинейность этой функции может быть измерена следующим образом:

$$P_f = \max_{0\neq a\in GF(2^k)} \max_{b\in GF(2^r)} \frac{\|\{x\in GF(2^k): f(x+a)-f(x)=b\}\|}{\|\{x\}\|},$$

где $\|\cdot\|$ есть количество элементов множества-аргумента. Величина P_f является показателем нелинейности функции: чем меньше её значение, тем выше нелинейность функции. Для линейных функций $P_f=1$.

Двоичная функция $f: GF(2^k)\to GF(2^r)$ называется совершенной нелинейной, если $P_f = 1/2^r$. Примером совершенной нелинейной функции является функция $f(x)=\sum_{i=1}^{s} x_{2i-1}\cdot x_{2i}$, отображающая элементы из поля $GF(2^{2sr})$ в поле $GF(2^r)$, где $x=(x_1x_2...x_{2s})\in GF(2^{2sr})$, $x_i\in GF(2^r)$. То есть, базисное разложение исходного вектора $x\in GF(2^{2sr})$ разбивается на $2s$ компонентов x_i, которые используются в качестве элементов меньшего поля $GF(2^r)$, после чего осуществляется суммирование результатов их попарного перемножения в поле $GF(2^r)$.

Совершенные нелинейные перестановки не существуют. В этом случае минимальное достижимое значение $P_f = 2/2^r = 2^{-r+1}$, такие функции называются почти совершенными нелинейными. Примерами таких функций являются: $f(x)=x^3$, $x\in GF(2^r)$ и $f(x)=x^{-1}$, $x\in GF(2^r)$, r – нечётное число.

Одним из классов нелинейных кодов, используемых для защиты от помех, являются надёжные коды, обнаруживающие ошибки. Они также называются *слабо защищёнными кодами, обнаруживающими алгебарические манипуляции* (weakly secure algebraic manipulation detection codes).

Код $C\in GF(2^n)$ называется R−надёжным, если мощность пересечения кода со всеми его сдвигами $\tilde{C}=\{\tilde{c}:\tilde{c}=y+e,\ c\in C,\ e\in GF(2^n),\ e\neq 0\}$ ограничен сверху величиной R:

$$R = \max_{0 \neq e \in GF(2^n)} \| \{c : c \in C, x + e \in C\} \| < \| C \|,$$

здесь и далее операции + и $\cdot$ есть аддитивная и мультипликативная операции в конечном поле, соответственно. Равномерно R−надёжным кодом называется код, размер пересечения которого со всеми сдвигами равен R. Легко заметить, что для линейных кодов $R = \| C \|$. Для краткости R−надёжные коды будем называть надёжными.

Таким образом, для каждой ненулевой ошибки e найдется не более R кодовых слов, прибавление ошибки к которым даст кодовые слова, то есть ошибка не будет обнаружена. Отсюда следует, что вероятность необнаружения ошибки кодом, мощность которого равна $\| C \| = M$, при условии равновероятности передаваемых сообщений ограничена снизу величиной $P_{\text{undet}} \leq R / M$. При $R < M$ код не имеет ошибок, которые гарантированно не будут обнаружены.

Примерами систематических 2−надёжных кодов являются следующие: $C_1 = \{(y \mid f(y) = y^3)\}$, $y \in GF(2^k)$ и $C_2 = \{(y \mid f(y) = y^{-1})\}$, где $y \in GF(2^k)$ − информационное сообщение; k − нечетное число; символом «|» обозначается конкатенация. Примером систематического 4−надёжного кода является следующий код: $C_3 = \{(y \mid f(y) = y^{-1})\}$, $y \in GF(2^k)$ $y \in GF(2^k)$ − информационное сообщение, k − чётное.

Принцип использования надёжных кодов в схемах параллельного обнаружения ошибок приведён на рисунке 4. Легко заметить, что он аналогичен использованию линейных кодов.

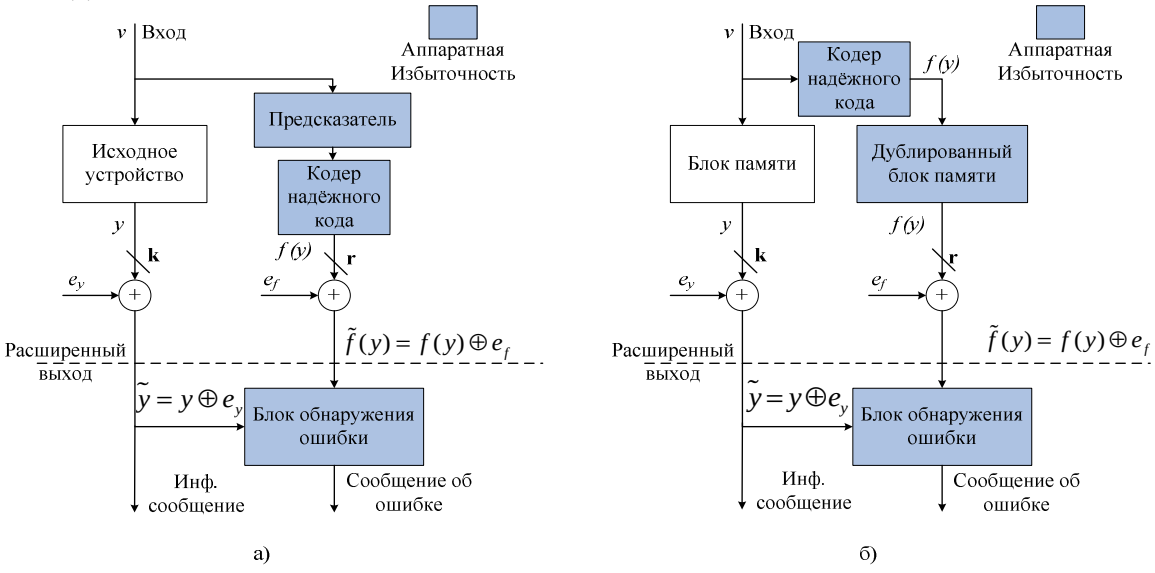

Рисунок 4.Схема использования надёжных кодов для параллельного обнаружения ошибок: а) для защиты линейных блоков вычислительных устройств; б) для защиты блоков памяти

Рассматривая надёжные коды относительно модели слабой алгебраической манипуляции, легко заметить, что, в отличие от линейных кодов, они не имеют необнаруживаемых ошибок. Для надёжных кодов не существует постоянной конфигурации необнаруживаемых ошибок. Например, при рассмотрении искусственной природы

помех получаем, что злоумышленник не может выбрать конфигурацию ошибок, которая с вероятностью, равной единице, будет успешно внедрена. Любая конфигурация ошибок не будет обнаружена с вероятностью $P^{w}_{\text{undet}} \le R/M$. Отсюда можно сделать вывод, что надёжные коды, обнаруживающие ошибки, гарантируют заданный уровень защищённости технических систем от слабых алгебраических манипуляций.

Однако надёжные коды не обеспечивают защиты от сильных манипуляций. Если зависимость между поступившими данными и возникающим искажением приводит к тому, что искажение принимает значение разности между текущим кодовым словом и любым другим, то такое искажение не может быть обнаружено. Следовательно, вероятность необнаружения сильной манипуляции $P^{s}_{\text{un det}} = 1$. Поэтому надёжные коды, обнаруживающие ошибки, не эффективны против ситуаций, описываемых моделью сильных алгебраических манипуляций.

Другим классом нелинейных кодов, используемым для защиты технических систем, являются *сильно защищённые коды, обнаруживающие алгебраические манипуляции* (strongly secure algebraic manipulation detection codes). Для краткости будем называть их кодами, обнаруживающими алгебраические манипуляции (algebraic manipulation detection code, AMD код). Данный класс кодов предназначен специально для защиты от сильных алгебраических манипуляций.

Очевидно, что для обеспечения заданного уровня защиты от сильных манипуляций процесс кодирования должен иметь недетерминированный характер. В противном случае при существовании определённого вида зависимости между входными данными и возникающим искажением гарантированно появление необнаруживаемых ошибок. Естественным путем решения этой проблемы является привнесение случайности в процесс кодирования, когда каждому сообщению соответствует множество кодовых слов, а выбор конкретного слова из этого множества определяется значением некоторой случайной величины, от которой не зависит величина искажения.

Для построения AMD кодов используются различные математические объекты: коды аутентификации, разностные структуры, помехоустойчивые коды и др. В работе приводятся примеры методов построения кодов на основе линейных помехоустойчивых кодов и операции умножения информационного и случайного компонентов кодового слова. Одним из наиболее исследованных и эффективных кодов является код, основанный на обобщённых кодах Рида–Маллера (также называемый кодом на основе полиномах). В работе приводится описание метода построения данного кода и его характеристики.

Кодовые слова систематического AMD кода представляют собой конкатенацию информационного сообщения $y \in GF(2^k)$, значения случайной величины $x \in GF(2^m)$ и значения нелинейной функции $f(y,x) \in GF(2^r)$:

$$C = \{(y \mid x \mid f(x,y))\}.$$

Сами коды, обнаруживающие алгебраические манипуляции, определяются как коды, для которых не существует такой конфигурации ошибок $e=(e_y \in GF(2^k),\ e_x \in GF(2^m),\ e_f \in GF(2^r))$ и такого значения y, при возникновении которых равенство

$$f(y,x)+e_f = f(y+e_y, x+e_x)$$

выполнится при всех возможных значениях x. Данное равенство, рассматриваемое как уравнение от неизвестной переменной x, называется уравнением маскирования ошибки (УМО). Легко заметить, что проверка выполнения этого равенства является аналогом вычисления синдрома принятого слова линейного кода. AMD код, определенный таким образом, будем называть AMD кодом в широком смысле.

AMD кодом в узком смысле будем называть код, для которого не существует такой конфигурации ошибок $e=(0 \neq e_y \in GF(2^k),\ e_x \in GF(2^m),\ e_f \in GF(2^r))$ и такого значения y, при возникновении которых равенство

$$f(y,x)+e_f = f(y+e_y, x+e_x)$$

выполнится при всех возможных значениях x. Другими словами, добавляется условие, что информационная часть кодового слова обязательно должна быть искажена: $e_y \neq 0$. AMD коды в узком смысле могут быть использованы во многих задачах, так как целью использования данного класса кодов является обеспечение целостности именно информационного сообщения.

Принцип использования кодов, обнаруживающих алгебраические манипуляции, в схемах с параллельным обнаружением ошибок представлен на рисунке 5.

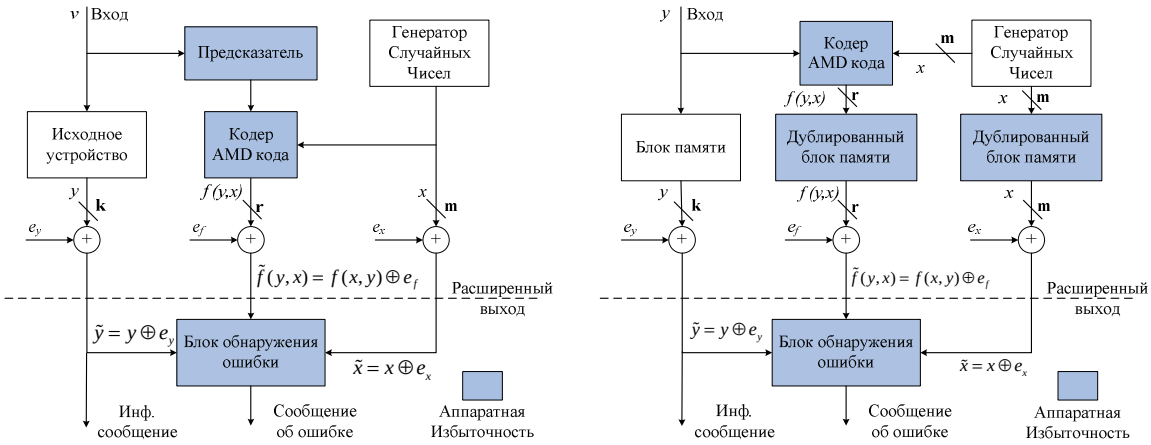

Рисунок 5.Схема использования кодов, обнаруживающих алгебраические манипуляции, для параллельного обнаружения ошибок: а) в линейных блоках вычислительных устройств; б) в блоках памяти

Согласно методу построения, данный класс кодов гарантирует заданный уровень защиты от сильных алгебраических манипуляций. Поскольку сильная модель является обобщением слабой модели манипуляций, AMD коды также обеспечивают защиту вычислительных устройств и от слабых манипуляций.

В третьей главе проводится теоретико-информационный анализ нелинейных кодов. Представлены границы, позволяющие оценить экстремальные значения параметров систематических надёжных кодов и кодов, обнаруживающих алгебраические манипуляции. Полученные автором границы позволяют оценивать оптимальность существующих методов построения кодов, задавая направления для дальнейших исследований.

Исследуем *минимальную длину (обозначим ее через* n*) систематического R-равномерно надёжного кода* над полем $GF(p^n)$. Пусть k – размерность кода, $M = p^k$ – мощность кода. В работе доказывается утверждение, что для систематического равномерно надёжного кода справедливо следующее неравенство:

$$n \geq \left\lceil \log_p \left(M^2 / R \right) \right\rceil.$$

Легко заметить, что данная граница также может быть применена и к неравномерно надёжным кодам. В этом случае происходит усиление неравенства:

$$n > \left\lceil \log_p \left(M^2 / R \right) \right\rceil.$$

При $p = 2$ и $R = 2$ граница приобретает следующий вид: $n \geq 2k - 1$. Можно показать, что существуют коды, лежащие на данной границе. При $k = 2$ ($n \geq 2k - 1 = 3$) примером кода, лежащего на этой границе, является следующий код: $C = \{(00|0), (01|1), (10|1), (11|1)\}$ над $GF(2^3)$. Данный код являются равномерно надёжным систематическим кодом с $R = 2$ и $P^w_{\text{undet}} = 1 - 2/4 = 0.5$, являясь при этом кодом с минимальной возможной длиной. Для сравнения, существующие конструктивные методы построения кодов над полем $GF(2^n)$ с $R = 2$ для любых k обеспечивают скорость $1/2$, то есть $n = 2k$. Таким образом, представленный код C для $k = 2$ обладает меньшей избыточностью при сохранении той же вероятности необнаружения ошибки $P^w_{\text{undet}} = 0.5$.

Данная граница может быть использована для оценки избыточности надёжных кодов. Условие применимости данной границы следующее: параметр *R* должен делить величину *M(M-1)* нацело и быть меньше величины *M*. Расхождения между представленной границей и существующими надёжными кодами показывают, что необходимы дальнейшие исследования на предмет существования более эффективных кодов и конструктивных методов их построения.

Вторая граница, представленная в данной главе, уточняет *вероятность необнаружения ошибки при использовании кодов, обнаруживающих алгебраические манипуляции, построенных на основе полиномов*. Рассмотрим вероятность необнаружения ошибки этим кодом. Определим величину $t = m/r$, при условии, что r делит m нацело. Напомним, что m бит это размер значения случайной величины x, а r бит – размер проверочных символов $f(x, y)$. Таким образом, мы делим величину x на t r-битных переменных.

Для любого (k, m, r) кода, обнаруживающего алгебраические манипуляции, где k – количество информационных символов; m – количество случайных символов; а r – количество проверочных символов, выполняется следующее неравенство:

$$P_{\text{undet}}(k,m,r) \geq 1 - d_q(2^m, M) \cdot 2^{-m},$$

где $d_q(2^m, M)$ - максимальное возможное расстояние Хэмминга q-ного ($q = 2^r$) кода длины 2^m и с $M = 2^{k+m+r}$ кодовыми словами.

Данную границу можно уточнить для всех кодов, построенных на основе обобщённых кодов РМ. В диссертационной работе приводится доказательство утверждения, что для AMD кодов на базе кодов Рида-Маллера справедлива следующая уточнённая нижняя граница:

$$P_{\text{undet}}(k,m,r) \geq 1 - (q - v^*)q^{-u^*-1},$$

где $u^* = \left\lfloor s^* / (q-1) \right\rfloor$; $v^* = s^* - (q-1)u^*$; $s^* = \min s_i : 1 - (q - v_i)q^{-u_i - 1} \geq 1 - d_q(2^m, M) \cdot 2^{-m}$; $s_i = 1, 2, \ldots$; параметры v_i, u_i вычисляются аналогично v^*, u^* для соответствующих s_i.

Полученная нижняя граница во многих случаях позволяет уточнить старую, более грубую границу. Она может быть использована для анализа кодов с точки зрения оптимальности в смысле обнаруживающей способности. Во многих случаях эта граница позволяет сделать вывод об оптимальности исследуемого кода, однако при некоторых значениях параметров k, m, r вероятность необнаружения ошибки конкретным кодом превышает значение уточнённой нижней границы. Из этого следует необходимость поиска новых методов построения кодов с более высокой обнаруживающей способностью, а также дальнейшее исследование их экстремальных характеристик.

В четвертой главе приведены новые кодовые методы повышения помехоустойчивости, представляющие интерес потому, что они уменьшают вычислительную сложность процедур кодирования и декодирования, а также увеличивают вероятность обнаружения алгебраических манипуляций.

Разработан кодовый метод на основе класса *обобщённых систематических надёжных (ОСН) кодов*, являющихся AMD кодами в широком смысле. Суть метода состоит в привнесении случайности в сообщение, кодируемое надёжным кодом. Это приводит к недетерминированности результата кодирования, когда каждому сообщению соответствует набор возможных кодовых слов. За счет этого устраняется уязвимость к сильным манипуляциям, характерная для надёжных кодов. Данный код является обобщением надёжных кодов для обнаружения сильных манипуляций. В работе приводится два метода построения ОСН кодов, один из которых основан на нелинейных перестановках в поле, а второй – на операции скалярного произведения.

Рассмотрим метод построения кода на основе перестановок. Пусть используется *R*-надёжный систематический код

$$C = \{(z \in GF(2^r) \mid f(z) \in GF(2^r))\},$$

где $f(z)$ − некоторая нелинейная перестановка в поле $GF(2^r)$. Пусть вектор z длины r бит представляет собой конкатенацию информационного сообщения $a \in GF(2^k)$ и случайного элемента $b \in GF(2^m)$, $r = k + m$. Тогда код можно представить как

$$C = \{(a \mid b \mid f(a \mid b))\}.$$

При $R < 2^m$ данный код является AMD кодом в широком смысле и обеспечивает вероятность необнаружения сильных алгебраических манипуляций, равную $P^s_{\text{undet}} \le R/2^m$. Вероятность необнаружения слабых манипуляций составляет $P^w_{\text{undet}} \le R/2^{(k+m)} = R/2^r$. Доказательства данных утверждений приведены в диссертационной работе. Легко заметить, что частным случаем ОСН кодов являются надёжные коды (при $m=0$). Рассмотрим пример построения ОСН кода. Пусть k=4, m=2, тогда $r = k+m$=6. В качестве функции кодирования выберем возведение в третью степень в поле Галуа: $f(x) = f(a,b) = (a \mid b)^3$. Таким образом, ОСН код строится на основе 2-надёжного кода $\{(z \mid z^3)\}$, $z \in GF(2^r)$. Итоговый код будет иметь скорость $k/(k+m+r) = 1/3$, гарантируя при этом вероятность необнаружения любой сильной манипуляции $P^s_{\text{undet}} \le 0.5$, а слабой – $P^w_{\text{undet}} \le 2^{-5} \approx 3 \cdot 10^{-2}$.

Кроме того, в работе описывается метод построения ОСН кода на основе кодирующей функции, являющейся операцией скалярного умножения в конечном поле:

$$C = \{(y \mid x \mid f(x,y) = \sum_{i=1,3,\ldots}^{t} (y_i \mid x_i)(y_{i+1} \mid x_{i+1}))\},$$

где $y \in GF(2^{at})$; $y = (y_1 \mid y_2 \mid \ldots \mid y_t)$; $y_i \in GF(2^a)$; $x \in GF(2^{bt})$; $x = (x_1 \mid x_2 \mid \ldots \mid x_t)$; $x_i \in GF(2^b)$; $f(x,y) \in GF(2^{a+b})$. Для данного кода $P^s_{\text{undet}} \le 2^{-b}$, $P^w_{\text{undet}} \le 2^{-(a+b)}$.

Метод построения обобщённого систематического надёжного кода позволяет спроектировать схему гибридного кодека, обнаруживающего алгебраические манипуляции. Принципиальная схема кодека представлена на рисунке 6.

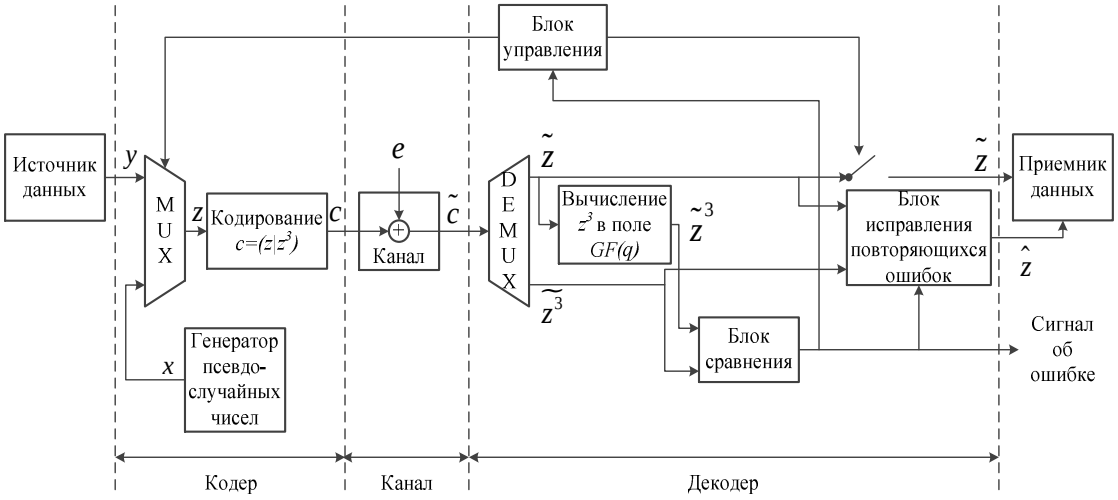

Рисунок 6. Принципиальная схема гибридного кодека, обнаруживающего алгебраические манипуляции.

Гибридный кодек работает по следующему принципу: используется кодек надёжного кода, однако в качестве кодируемого сообщения поступает конкатенация информационных и случайных символов. Описанная схема кодека позволяет динамически менять скорость кода за счет увеличения/уменьшения доли случайных символов в зависимости от ситуации в канале или же от значимости данных. Кодек обеспечивает требуемый уровень обнаружения ошибок для различных блоков устройства и

заменяет несколько различных кодеков надёжных кодов и кодов, обнаруживающих алгебраические манипуляции, снижая требуемые аппаратные затраты.

Положенный в основу кодового метода надёжный код позволяет применять к ОСН кодам алгоритмы, разработанные для надёжных кодов, например, алгоритм исправления повторяющихся ошибок. По аналогии с процедурой исправления повторяющихся ошибок с помощью надёжных кодов, ОСН коды способны исправлять ошибки, если они встречаются в течение трёх и более тактов работы устройства.

Кроме того, в диссертационной работе предлагается *алгоритм обнаружения и исправления ошибок малой кратности для обобщённых систематических надёжных кодов на основе перестановок в поле*. Надёжные и AMD коды зачастую обладают минимальным расстоянием, равным единице. Увеличение минимального расстояния приводит к улучшению обнаруживающих и корректирующих характеристик кода, что приводит к росту достоверности кодируемых данных. Для коррекции ошибок прежде всего требуется увеличение минимального расстояния кода до трёх и более. В работе предлагается увеличивать расстояние за счёт кодирования компонентов слова ОСН кода линейным кодом, например, кодом с проверкой на чётность. Приводятся две модификации ОСН кода, расстояния которых не менее трёх и четырёх, соответственно. Код с расстоянием три может быть представлен следующим образом:

$$C = \{(y \mid x \mid f(x, y) \mid p(y) = wt(y) \bmod 2)\},$$

где через $wt(y)$ обозначен вес Хэмминга вектора y. Для каждого из кодов в диссертационной работе представлен вычислительно простой метод декодирования. Алгоритм декодирования заключается в выборе результата декодирования из информационного сообщения и прообраза кодирующей функции в зависимости от выполнения проверки на чётность.

Таким образом, демонстрируется возможность использования ОСН кодов в качестве кодов, исправляющих однократную ошибку, и кодов, исправляющих однократную и обнаруживающих двукратную ошибки. Алгоритмы декодирования используют дистанционные характеристики как линейных кодов, так и самих ОСН кодов, что приводит к снижению требуемой информационной избыточности. Вычислительная сложность алгоритмов уменьшается за счёт обратимости кодирующей функции, что позволяет использовать её прообраз в процессе декодирования. Вычислительная сложность представленных алгоритмов ниже, чем у соответствующих алгоритмов для других кодов.

При фиксированных размерах информационного сообщения и значения случайной величины скорость получаемого кода оказывается ниже, чем у кодов, основанных на полиномах. Однако при фиксированном размере значения случайной величины предлагаемый код обеспечивает максимальную вероятность обнаружения манипуляций среди AMD кодов в широком смысле. Кроме того, простота метода построения кода, возможность использования гибридного кодека, обнаруживающего манипуляции, а также вычислительно эффективные алгоритмы исправления повто-

ряющихся ошибок и ошибок малой кратности являются значительными преимуществами класса обобщённых систематических кодов.

В качестве базового надёжного кода для построения ОСН кодов предлагается разработанный автором *систематический 2-надёжный код, основанный на экспоненциальной функции*. Пусть информационное сообщение x есть элемент абелевой группы $G\{0, ..., p-1\}$ (p – простое число), тогда код

$$C = \{(x \mid u^x \bmod p)\},$$

где u есть примитивный элемент поля $GF(p)$, является систематическим надежным кодом с $k = \lceil \log_2 p \rceil$, $n = 2k$ и $R = 2$.

Предлагаемый надёжный код на основе экспоненциальной функции позволяет обеспечивать гарантированное обнаружение слабых алгебраических манипуляций. Более того, данный код обеспечивает защищённость данных от асимметричных ошибок с битовыми переходами вида ($0 \rightarrow 0$, $1 \rightarrow 0$) и ($1 \rightarrow 0$, $1 \rightarrow 1$). Появление асимметричных ошибок характерно для многих современных типов памяти. Существующие надёжные коды не обеспечивают защиту от асимметричных ошибок.

Также, в данной главе предлагаются *модификации известного кодового метода с использованием AMD кода в узком смысле, основанного на операции умножения информационного и случайного компонентов кодового слова*. Код обладает простым методом построения, обеспечивая при этом максимально возможную вероятность обнаружения сильных манипуляций. Код выглядит следующим образом:

$$C = \{(y \mid x \mid f(x, y) = x \cdot y)\},$$

где $y, x, f(y, x) \in GF(2^k)$ (то есть $m = r = k$), операция умножения выполняется в поле $GF(2^k)$. Вероятность успешного проведения сильных и слабых манипуляций при $e_y \neq 0$ составляет $P^w_{\text{undet}} = P^s_{\text{undet}} = 2^{-k}$. Основным недостатком данного метода построения кода является отсутствие гибкости при выборе параметров. Размер информационного сообщения k полностью определяет длину кода $n = 3k$, размер значения случайной величины – k бит, а также вероятность необнаружения ошибки $P^w_{\text{undet}} = P^s_{\text{undet}} = 2^{-k}$. В диссертационной работе предлагаются две модификации метода построения кода, которые позволяют варьировать размер значения случайной величины и, как следствие, скорость кода и вероятность обнаружения манипуляций.

Модификация на основе расширения случайной величины основана на использовании в процессе кодирования значения случайной величины x из меньшего конечного поля $GF(2^m)$, $m < k$. Для выполнения умножения в поле значение величины x расширяется до k бит нулями, после чего выполняются действия в соответствии с оригинальным методом построения кода. Данная модификация позволяет изменить скорость кода с $1/3$ до $k/(2k+m)$, обеспечивая вероятность необнаружения сильных и слабых манипуляций $P^s_{\text{undet}} = P^w_{\text{undet}} \leq 2^{-m}$. Доказательство данного утверждения приведено в диссертационной работе.

Модификация на основе разбиения информационного сообщения заключается в делении кодируемого сообщения $y \in GF(2^{u \cdot m})$ на u блоков $y_i \in GF(2^m)$. Эти блоки

подвергаются процедуре кодирования в соответствии с оригинальным методом построения кода на фиксированном значении случайной величины x, после чего объединяются в кодовое слово c по следующему правилу:

$$c = (y_1 \mid y_2 \mid ... \mid y_u \mid x \mid y_1 \cdot x \mid y_2 \cdot x \mid ... \mid y_u \cdot x).$$

При декодировании происходит обратное разделение слова c на u промежуточных слов, каждое из которых проверяется на наличие ошибок. При условии, что наличие ошибки хотя бы в одном информационном блоке y_i приводит к принятию решения о некорректности всего вектора y, данный код гарантирует вероятность успешного проведения сильных и слабых манипуляций $P^s_{\text{undet}} = P^w_{\text{undet}} \le 2^{-m}$. Доказательство данного утверждения приведено в диссертационной работе. Описанная модификация позволяет менять размер значения случайной величины, длины кода и вероятности обнаружения ошибок аналогично модификации на основе расширения случайного числа. Кроме того, данная модификация позволяет значительно уменьшить аппаратные затраты на реализацию кодека. Стоит отметить, что принцип разбиения информационного сообщения является применимым для различных классов кодов, обнаруживающих алгебраические манипуляции (например, для ОСН кодов).

Четвёртая глава диссертационной работы завершается описанием *кодового метода повышения помехоустойчивости с использованием AMD кода в узком смысле, основанного на операции скалярного умножения компонентов информационного сообщения и значения случайной величины*. Суть данного метода состоит в разбиении сообщения $y \in GF(2^{sr})$ и значения случайной величины $x \in GF(2^{sr})$ на блоки размера r бит с их последующим перемножением в поле $GF(2^r)$. Результаты умножений складываются, формируя проверочный символ. Легко заметить, что, разбивая y и x на один блок, получаем код, основанный на операции умножения информационного и случайного компонентов кодового слова, рассмотренный выше, который является частным случаем данного метода построения кода.

Рассмотрим код

$$C = \{(y \mid x \mid f(x, y) = \sum_{i=1}^{s} x_i \cdot y_i)\},$$

где $y,\ x \in GF(2^{sr})$, $y_i,\ x_i,\ f(x, y) \in GF(2^r)$, $i = 1, ..., s$. Данный код является AMD кодом в узком смысле и не обнаруживает манипуляции, описываемые слабой и сильной моделями, с вероятностью $P^s_{\text{undet}} = P^w_{\text{undet}} = 2^{-r}$ при условии, что $e_y \neq 0$. Доказательство утверждения приведено в диссертационной работе.

Предлагаемый код при фиксированных параметрах k, m, r обеспечивает большую вероятность обнаружения манипуляций, нежели коды, основанные на полиномах. При этом функция вычисления проверочных символов данного кода имеет меньшую степень и меньшее количество мономов, что ведет к значительному уменьшению вычислительной сложности процедур кодирования и декодирования. По сравнению с AMD кодами на основе линейных помехоустойчивых кодов данный метод построения кодов обеспечивает гибкость в выборе параметров. Применение этого ко-

да приводит к улучшению обнаруживающих характеристик, а также снижает сложность процедур кодирования и декодирования.

Пятая глава посвящена научно-техническим предложениям по применению разработанных кодовых методов. Рассматриваются два приложения:

1. Повышение достоверности информации в бортовых накопителях космических аппаратов с длительным периодом эксплуатации на высоких орбитах.
2. Повышение надёжности обработки информации аппаратной реализацией шифра AES.

Проведённые расчёты показали, что использование предлагаемых методов помехоустойчивого кодирования позволяет гарантировать заданный уровень надежности обработки и хранения информации при условии непредсказуемых потоков ошибок, характерных для данных приложений исследуемой модели канала.

В заключении представлена итоговая оценка проделанной работы и приведены основные результаты проведенного исследования и их соотношение с целью и задачами, научной новизной, практической значимостью и положениями, выносимыми на защиту, которые поставлены и сформулированы во введении. **В приложении** приведён анализ атак по сторонним каналам, позволяющий оценить степень опасности различных атак для реализаций криптографических алгоритмов.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. В работе предложены новые кодовые методы обеспечения целостности данных для каналов, описываемых моделью канала с алгебраическими манипуляциями. Показано, что использование предлагаемых методов и алгоритмов позволяет увеличить вероятность обнаружения манипуляций и уменьшить вычислительную сложность процедур кодирования и декодирования, что, в свою очередь, повышает достоверность обработки и передачи информации вычислительными устройствами.

2. Полученные результаты можно сформулировать следующим образом:

- Разработка и исследование кодового метода повышения помехоустойчивости на основе класса обобщённых систематических надёжных кодов, обнаруживающих алгебраические манипуляции.
- Разработка алгоритма обнаружения и исправления ошибок малой кратности с помощью обобщённых систематических надёжных кодов.
- Разработка и исследование кодового метода повышения помехоустойчивости, основанного на операции скалярного умножения компонентов информационного сообщения и значения случайной величины.
- Осуществление модификаций кодового метода, основанного на операции умножения информационного и случайного компонентов, с целью уменьшения информационной избыточности.

- Вывод оценок экстремальных значений параметров нелинейных кодов, обнаруживающих алгебраические манипуляции.

Таким образом, решены все задачи, поставленные для достижения сформулированной в работе цели.

3. Показано, что преобразование данных с использованием предлагаемых кодовых методов зачастую обеспечивает более высокий уровень защиты от алгебраических манипуляций, нежели использование существующих решений. Кроме того, алгоритмы декодирования некоторых кодов обладают меньшей вычислительной сложностью, что приводит к снижению затрат на их реализацию по сравнению с аналогами. Использование предлагаемых методов помехоустойчивого кодирования позволяет повысить надёжность обработки информации и качество функционирования технических систем. Таким образом, цель работы достигнута.

4. На основе решённых в диссертации задач можно определить следующие направления дальнейших исследований:

- Разработка методов построения систематических надёжных кодов, обладающих минимальной избыточностью.
- Разработка алгоритма исправления ошибок малой кратности для кодов, основанных на операции скалярного умножения компонентов информационного сообщения и значения случайной величины.
- Исследование возможности построения систем связи с обратной связью на основе надёжных кодов.
- Разработка и исследование нелинейных кодовых методов с простыми алгоритмами кодирования и декодирования (с низким энергопотреблением) для бортовых систем обработки информации аэрокосмических систем и комплексов.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. **Громова, А. Н. Вариант алгоритма нахождения ошибок для БЧХ-кодов [Текст] / А.Н. Громова, М.О. Алексеев // Программные продукты и системы – Тверь: МНИИПУ. – 2010. – №2 (май). – С. 56-58.**
2. **Алексеев, М.О. Нижняя граница длины систематических равномерно надежных кодов [Текст] / М.О. Алексеев // Известия ВУЗов. Приборостроение. №8 (август), 2013. – С. 14-16.**
3. **Алексеев, М.О. Новая конструкция систематического надежного кода [Текст] / М.О. Алексеев // Известия ВУЗов. Приборостроение. – 2013. − №8 (август). − С. 24-27.**
4. **Алексеев, М.О. Об обнаружении алгебраических манипуляций с помощью операции умножения [Текст] / М.О. Алексеев // Информационно-управляющие системы. – 2014. – № 3 (июнь). – С. 103-108.**

5. **Алексеев, М.О. Защита от алгебраических манипуляций на основе операции скалярного умножения [Текст] / М.О. Алексеев // Проблемы информационной безопасности. Компьютерные системы. – 2014. – №2. – С. 47-53.**
6. Алексеев, М.О. Об обнаружении ошибок с помощью нелинейных кодов [Текст] / М.О. Алексеев, Е.Т. Мирончиков // Научная сессия ГУАП: Сб. докл.: В 3 ч. Ч. I. Технические науки / СПб.: ГУАП. – 2011. – С. 40-43.
7. Алексеев, М.О. Уточненная нижняя граница обнаруживающей способности AMD кодов [Текст] / М.О. Алексеев // Научная сессия ГУАП: Сб. докл.: В 3 ч. Ч. I. Технические науки / СПб.: ГУАП. – 2012. – С. 61-64.
8. Алексеев, М.О. Пакетная передача с кодовым зашумлением. Теоретические основы и практическое применение [Текст] / М.О. Алексеев. – LAP LAMBERT Academic Publishing, 2012. – 57 с. – ISBN: 978-3-8484-1675-2.
9. Алексеев, М.О. Обобщение надежных кодов [Текст] / М.О. Алексеев, А.В. Еганян // СПИСОК-2013: Материалы всероссийской науч. конф. по проблемам информатики. – СПб.: Издательство ВВМ. – 2013. – С. 263-268.
10. Алексеев, М.О. О гибридном кодеке, обнаруживающем алгебраические манипуляции [Текст] / М.О. Алексеев // Научная сессия ГУАП: Сб. докл.: В 3 ч. Ч. I. Технические науки / СПб.: ГУАП. – 2013. – С. 3-6.
11. Алексеев, М.О. Об исправлении ошибок малой кратности обобщёнными систематическими надёжными кодами [Текст] / М.О. Алексеев // Теория и практика современной науки: материалы XV Междунар. научно-практической конф., г. Москва, 8–9 октября 2014 г. / Науч.-инф. издат. центр «Институт стратегических исследований». – М.: Изд-во «Институт стратегических исследований». – 2014. – С. 47-53.
12. Alekseev, M. Two Algebraic Manipulation Detection Codes Based on a Scalar Product Operation [Текст] / M. Alekseev // Proc. of the Workshop on Coding and Cryptography (WCC). – 2015.

Формат 60x84 1/16. Бумага офсетная. Печать офсетная.
Тираж экз. Заказ № .