ОТЗЫВ

официального оппонента на диссертацию

Алексеева Максима Олеговича

«Методы нелинейного кодирования для повышения достоверности обработки информации», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.01 – «Системный анализ, управление и обработка информации (технические системы)».

Актуальность темы исследования

Диссертационная работа М.О. Алексеева «Методы нелинейного кодирования для повышения достоверности обработки информации» посвящена разработке и исследованию методов повышения помехоустойчивости функционирования вычислительных устройств, подвергающихся алгебраическим манипуляциям.

Для каналов, которые можно описать относительно простыми моделями, например, классической моделью канала с шумом, задача построения помехоустойчивых кодов, согласованных с шумом, является хорошо изученной. Для них разработаны различные классы линейных помехоустойчивых кодов, обеспечивающих гарантированное повышение надёжности передачи, хранения и обработки информации при относительно невысокой сложности их реализации и при достижении эффективности близкой к теоретическим пределам.

Построение эффективных методов повышения достоверности в ситуациях, описываемых более сложными явлениями, зачастую является трудновыполнимой задачей. В качестве одного их возможных решений этой задачи является использование методов преобразования исходного канала в канал, согласованный с корректирующими свойствами известных кодовых методов. Однако такие преобразования были разработаны не для всех каналов, что сужает область их применения.

Другим методом повышения помехоустойчивости в сложных каналах, не требующих решения задачи согласования потока ошибок и корректирующей способности кода, является использование нелинейных кодовых методов, обнаруживающих любые помехи, вызванные ионизирующими излучениями, старением электронных элементов, целенаправленным физическим воздействием злоумышленника. Эти кодовые методы обладают близкой к равномерной обнаруживающей способностью. Их применение позволяет гарантировать заданный уровень обнаружения любых помех, обеспечивая надёжное функционирование технических систем в большом многообразии каналов.

Кодовые методы, разрабатываемые и исследуемые в работе Алексеева М. О., направлены на повышение помехоустойчивости в каналах, описываемых моделью канала с алгебраическими манипуляциями. Данная модель может быть использована для описания достаточно большого класса реальных каналов, примеры которых подробно описаны в диссертационной работе. Решаемая задача построения кодовых методов повышения помехоустойчивости для каналов с алгебраическими манипуляциями является актуальной и востребованной на практике.

Степень обоснованности научных положений, выводов и рекомендаций

Автор достаточно корректно использует известные научные методы обоснования положений, выводов и рекомендаций других авторов в области построения методов помехоустойчивого кодирования. Для обоснования полученных результатов, выводов и положений Алексеев М. О. корректно использует известные научные методы, адекватные природе исследуемых процессов и явлений.

Теоретическая состоятельность работы подтверждается непротиворечивостью полученных в исследовании результатов, данным, представленным в известных работах по нелинейным методам кодирования Ю. Васильева, Ф. Соловьевой, К. Фелпса. М. Карповского и др.

Основные результаты диссертации неоднократно обсуждались на различных конференциях и получили одобрение специалистов.

Научная новизна и достоверность результатов

Научная новизна работы состоит в разработке и исследовании методов повышения помехоустойчивости функционирования вычислительных устройств на основе нелинейного кодирования. Основные результаты получены автором путем применения вычислительно простых нелинейных функций в качестве кодирующих функций, используемых для вычисления проверочной части кодового слова. Основными результатами диссертационной работы являются:

1. Кодовый метод повышения помехоустойчивости, основанный на классе обобщённых систематических надёжных кодов (AMD-кодов). Научная новизна данного метода заключается в привнесении случайности в процесс кодирования надёжных кодов, что позволяет использовать получаемые обобщённые надёжные коды для обнаружения помех, описываемых моделью как слабых, так и сильных манипуляций. При этом обеспечивается более высокая вероятность обнаружения помех, описываемых

моделью слабых манипуляций. При некоторых параметрах данный кодовый метод может достигать большей вероятности обнаружения помех, чем известные методы.

В диссертационной работе также рассматривается возможность применения гибридного кодека (реализации кодера и декодера обобщённого систематического надёжного кода), позволяющего динамически изменять скорость кодирования в зависимости от уровня сигнал/шум в канале. Использование подобной реализации кодека может привести к снижению затрат на обеспечение помехоустойчивости технической системы.

В качестве одного из надёжных кодов, который может быть выбран в качестве базового для построения обобщённого систематического надёжного кода, в диссертационной работе предлагается надёжный код на основе экспоненциальной функции. Показывается, что предлагаемая кодирующая функция является почти совершенной нелинейной функцией и при определённых параметрах по обнаруживающей способности близка к лучшим известным кодам. В то же время, применение этой функции позволяет обеспечить защищённость технических систем от асимметричных ошибок, характерных для некоторых типов каналов. Известные кодовые методы не обеспечивают гарантированное обнаружение асимметричных ошибок.

По сравнению с аналогами данный метод также обладает вычислительно простыми алгоритмами исправления повторяющихся ошибок и ошибок малой кратности. Однако стоит отметить, что информационная избыточность данного кода зачастую выше, чем у аналогов, поэтому его применение может быть целесообразно при отсутствии строгих ограничений на избыточность, позволяя при этом использовать схему гибридного кодека и простые процедуры исправления ошибок.

2. Алгоритм обнаружения и исправления ошибок малой кратности для обобщённых систематических надёжных кодов. В работе подробно рассматривается способ увеличения минимального расстояния обобщённых надёжных систематических кодов до трёх и четырёх путём добавления проверок на чётность определённых частей кодового слова. За счёт этого автор компенсирует невысокое минимальное расстояние, характерное для рассматриваемых классов кодов, при котором не может быть осуществлено исправление даже однократных ошибок. В результате получаются коды, содержащие как нелинейные, так и линейные проверочные символы, увеличивающие минимальное кодовое расстояние, что позволяет обнаруживать и исправлять ошибки малой кратности.

Алгоритм, основан на обратимости кодирующей функции и использовании для увеличения кодового расстояния не только линейных, но и нелинейных компонент кодового слова. В работе приводится сравнение алгоритма с аналогичным алгоритмом для кодов на основе обобщённых кодов Рида-Маллера, из которого следует, что предлагаемый алгоритм обладает меньшими информационной избыточностью и вычислительной сложностью.

3. Кодовый метод повышения помехоустойчивости, основанный на операции скалярного умножения компонентов информационного сообщения и значения случайной величины. Основное преимущество данного по сравнению с кодами на основе Рида-Маллера заключается в том, что он является AMD кодом в узком смысле. Это позволяет использовать более простую кодирующую функцию, которая является линейным полиномом. При этом достигается вероятность необнаружения помех, минимум в два раза меньшая, чем для кодов на основе кодов Рида-Маллера. По сравнению с кодами на основе операции умножения и на основе линейных помехоустойчивых кодов предлагаемый метод позволяет строить коды с различными параметрами.

   Необходимо также отметить, что код на основе операции умножения является частным случаем предлагаемой конструкции, что позволяет считать её обобщением известного кодового метода на основе умножения.

4. Две модификации кодового метода на основе операции умножения. Модификации позволяют варьировать параметры кода (размер случайной величины, вероятность обнаружения помех, скорость кода), адаптируя их к непосредственным требованиям технической системы. Исходная кодовая конструкция не позволяет варьировать параметры кода, они напрямую определяются длиной кодируемого сообщения. Предлагаемые модификации основаны на расширении случайной величины и на разбиении информационного сообщения. Обе модификации обеспечивают аналогичную вероятность обнаружения помех, определяемую размером случайной величины.

5. Две нижние границы параметров нелинейных кодов.

   Нижняя граница вероятности необнаружения алгебраической манипуляции применима к AMD кодам на основе кодов Рида-Маллера и позволяет оценивать их оптимальность в смысле обнаруживающей способности. Граница является уточнением общей границы для кодов, обнаруживающих алгебраические манипуляции, полученной за счёт использования конкретных дистанционных характеристик кодов Рида-Маллера.

Нижняя граница длины систематического равномерно надёжного кода является уточнением границы для несистематических кодов и демонстрирует минимальное значение длины кода при заданных параметрах. Данная граница является достижимой, в работе приводится пример кода, лежащего на ней. В работе также демонстрируется вид этой границы для неравномерно надёжных кодов.

Представленные результаты не противоречат практике и накопленному опыту в области помехоустойчивого кодирования, не противоречат результатам других авторов. Параметры некоторых предлагаемых кодовых методов лежат на теоретической границе, что подтверждает корректность методов.

Теоретическая значимость результатов

Теоретическая значимость диссертационного исследования Алексеева М. О. заключается в развитии теории помехоустойчивого кодирования за счёт разработки новых методов построения нелинейных кодов. Большую теоретическую ценность имеют полученные в работе оценки параметров кодов и оценки вероятностей необнаружения алгебраических манипуляций.

Практическая значимость результатов

Практическая значимость результатов диссертационного исследования Алексеева М. О. заключается в том, что разработанные методы повышения помехоустойчивости, в силу присущей им простоты, могут быть эффективно использованы для борьбы с алгебраическими манипуляциями в широком диапазоне реальных условий обработки информации (проектирование помехозащищенной памяти, аппаратная реализация вычислительных устройств, устойчивых к привносимым помехам, системы передачи данных с обратной связью, нечеткие экстракторы и др.)

Внедрение результатов

Результаты диссертационного исследования были успешно внедрены ЗАО «Научные приборы» при исследовании и разработке методов проектирования надёжных электронных документов. Кроме того, результаты были использованы в СПбГУАП при проведении научно-исследовательской работы по разработке алгоритмов повышения помехоустойчивости твердотельной памяти бортовых комплексов космических аппаратов. Также, результаты диссертационной работы были использованы при организации учебной деятельности СПбГУАП.

Полнота публикаций научных результатов

Диссертация написана грамотным языком, хорошо структурирована и подробно освещает основные и промежуточные результаты исследования. Основное содержание диссертации достаточно полно отражено в 12 печатных работах автора, в том числе в 5 статьях в журналах, входящих в список ВАК. Основные результаты апробированы на международных и всероссийских конференциях.

Автореферат правильно и в достаточной мере отражает содержание диссертационной работы.

Замечания по диссертации

Необходимо отметить следующие замечания по диссертационной работе:

1. В работе не приводится информация о кодовых методах обнаружения алгебраических манипуляций на основе кодов аутентификации и разностных структурах. Также не проведена связь с методами случайного кодирования в рамках вайнеровской концепции «подслушивающего канала».
2. Не исследуется вопрос возможности построения обобщённых систематических частично надёжных кодов. Вопрос возможности уменьшения размера проверочной части кодового слова для данной конструкции является весьма актуальным.
3. Формулировка, что «код не имеет необнаруживаемых ошибок» представляется не совсем точной, так как всегда существуют ошибки, переводящие одно кодовое слово в другое, то есть, фактически, необнаруживаемые. В данном случае более корректно было бы использовать следующую формулировку: «код не имеет постоянной конфигурации необнаруживаемых ошибок для всех кодовых слов».
4. В разделе 4.1.3 описывается алгоритм исправления повторяющихся ошибок, при этом не приводятся примеры ситуаций, приводящих к возникновению повторяющихся ошибок.
5. Модификация кодового метода на основе операции умножения информационного и случайного компонентов, основанная на разбиении информационного сообщения, описанная в разделе 4.3.3, может быть аналогично применена и к обобщению данного метода – коду на основе операции скалярного кодирования, однако в диссертационной работе автор не указывает на это обстоятельство.
6. В работе представлены два научно-технических предложения по практическому применению нелинейных кодовых методов. Первое из них относится к повышению надежности обработки информации в бортовых вычислительных комплексах космических

аппаратов, что само по себе усиливает и конкретизирует практическую ценность работы. Однако второе предложение, нацеленное на защиту архитектуры шифра AES, выглядит, на наш взгляд, странным. Целесообразно было бы вместо шифра AES, рассматривать российский шифр ГОСТ 28147-89 и его перспективный аналог.

Стоит отметить, что перечисленные замечания не ставят под сомнение новизну, теоретическую и практическую значимость результатов диссертационной работы, полученных автором лично.

Заключение

В работе изложены результаты исследования, имеющие большое значение для развития теории помехоустойчивого кодирования, в частности нелинейных методов кодирования, что обеспечивает построения надёжных технических систем, обладающих высоким уровнем помехозащищённости в каналах с алгебраическими манипуляциями. Исходя из содержания исследования, можно сделать вывод, что диссертация является законченной научно-исследовательской работой, выполненной автором самостоятельно на высоком научном уровне. Результаты работы обладают научной новизной, а их внедрение свидетельствует о практической значимости работы.

Работа М.О. Алексеева отвечает требованиям п. 9 Положения о присуждении ученых степеней, утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 № 842, предъявляемым к кандидатским диссертациям, а автор заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.01 – «Системный анализ, управление и обработка информации (технические системы)».

Доктор технических наук, профессор,
профессор кафедры «Защищённые системы связи»
Санкт-Петербургского государственного университета
телекоммуникаций имени профессора М. А. Бонч-Бруевича В. А. Яковлев
«10» сентября 2015г.