УДК 004.056.5

КРЫЛОВА В.А., к.т.н.,
МИРОШНИК А.Н., студент (НТУ «ХПИ»)

Разработка методов оценки эффективности систем защиты информации в распределенных компьютерных системах

Статья посвящена разработке и усовершенствованию методов, средств защиты, обработки и передачи информации, оценки эффективности систем защиты информации в распределенных информационных системах специального назначения. Проведен анализ существующих методов и средств адаптивной защиты информации в цифровых системах связи. Предложено решение задачи оперативного нахождения параметров помехоустойчивого кода. Разработан метод определения качества канала связи на основе оценке статистических характеристик потока ошибок.

В статье предложена технология синтеза сигнально-кодовых конструкций на основе системы сигналов с гребенчатым спектром и адаптивным кодированием. Предложен алгоритм нахождения коэффициентов цифровых фильтров для реализации системы уплотнения сигналов методами условной минимизации переходных помех между объединяемыми сигналами.

Ключевые слова: *компьютеризированные системы и сети, система защиты информации, адаптивное кодирование, широкополосные сигналы, сигнально-кодовые конструкции, гребенчатый фильтр.*

Введение

Современное развитие вычислительной техники и элементной базы способствует дальнейшему развитию информационных автоматизированных систем управления (АСУ), основанных на цифровой обработке, защиты и передачи информации. Скорость обмена данными и их объем непрерывно увеличивается наряду с увеличением области применения компьютеризированных систем и сетей. Это в свою очередь ведет к росту числа дестабилизирующих факторов, в том числе возрастанию влияния помех при передаче сигналов.

Вопросы оптимизации процесса защиты и передачи информации являются важной задачей, как для сфер государственного управления, банковской деятельности, управления технологическим процессами на предприятиях, управления транспортными средствами, так и для военного сектора. В современных условиях, когда внедряются новые формы ведения военных действий, основанные на использовании сетецентрического способа управления войсками, роль и значение единой автоматизированной системы управления значительно возрастает. Компьютеризированная интегрированная система вооруженного противоборства с интеграцией всех участников боевых действий в единую информационную сеть, должна быть обеспечена быстродействующими аппаратно-программными модулями. Основной задачей компьютерных компонентов АСУ является обеспечения надежного доведения сообщений и команд управления в установленное время с заданной достоверностью в сложной помеховой обстановке.

Возрастающие требования к оперативности и своевременности передачи данных в специализированных компьютерных системах и сетях военного назначения в сочетании с жесткими требованиями к вероятностно-временным характеристикам доведения информации требуют усовершенствования и разработки аппаратно-программных средств обработки, защиты и передачи информации.

Надежность передачи информации в компьютеризированных интегрированных системах обеспечивается использованием различных видов помехоустойчивого кодирования, которое отличается от других методов тем, что полностью реализуется на элементах цифровой техники: микроконтроллерах, программируемых логических интегральных схемах (ПЛИС), что делает кодовые методы защиты информации менее энергоемкими, менее габаритными и более дешевыми.

При выборе помехоустойчивого кода его параметры необходимо согласовывать с источником сообщения, каналом связи и требованиями, предъявляемыми к доведению сообщения. Процедура выбора помехоустойчивого кода, а также параметров кодера, для соответствующего канала связи, осуществляется на этапе разработки и проектирования информационной системы, исходя из предполагаемых характеристик канала. Однако в реальных условиях

состояние информационного канала обусловлено нестабильностью его параметров, зависящей не только от наличия других источников полезного сигнала, но и от погодных, климатических и других причин. При этом характеристики канала динамически изменяются с течением времени, что приводит к недостаточно эффективному использованию пропускной способности информационного канала, в случае если параметры системы защиты выбираются однократно, без возможности их адаптации к условиям функционирования.

Такой подход к выбору кода для реальных каналов приводит, как правило, к уменьшению скорости передачи информации из-за нерационального использования избыточности в каждом из возможных состояний информационного канала. Поэтому при построении компьютеризированных информационных систем и сетей возникает необходимость разработки универсальных модулей защиты и передачи информации, за счет применения новых технологий помехоустойчивого кодирования, важным направлением которого является адаптивное кодирование.

Реализация универсальных аппаратно-программных средств защиты информации ограничивается многими факторами, в том числе зависимостью параметров алгоритмов кодирования от параметров системы передачи, а также критичностью к аппаратным и программным ресурсам системы. Использование динамически реконфигурируемых ПЛИС в компьютеризированных интегрированных системах, позволяет интегрировать программную и аппаратную реализацию унифицированных методов и алгоритмов защиты информации, обеспечив высокую степень достоверности и скорости передачи.

При использовании адаптивных методов защиты информации в цифровых сетях связи важным является вопрос выбора в качестве переносчика закодированной информации сигнально-кодовой конструкции (СКК). Одним из подходов, использующихся для повышения помехоустойчивости в условиях сосредоточенных по спектру помех, является использование СКК, обладающих расширенным энергетическим спектром. Однако распределение энергетических составляющих в частотной области существующих широкополосных сигналов не позволяет повысить помехоустойчивость информационных сетей при воздействии сосредоточенных по спектру помех за счет расширения спектра СКК.

Постановка проблемы в общем виде и ее связь с важными научными или практическими задачами

Разработка и усовершенствование аппаратно-программного обеспечения обработки, защиты и передачи информации в компьютеризированных интегрированных системах и сетях с унифицированными методами защиты информации, которые выполняют процедуру адаптации и отвечают требованиям минимальных аппаратных и энергетических затрат, является актуальной научно-практической задачей.

Анализ последних исследований и публикаций, в которых начато исследование универсальных методов защиты информации и особенностей их реализации

В настоящее время при выборе помехоустойчивого кодера его параметры должны быть согласованы с источником сообщения, каналом связи, а также требованиями, предъявляемыми к достоверности доведения информации до получателя. Однако сложно заранее выбирать параметры кода, если качество канала связи неизвестно, а иногда вообще оно может изменяться в процессе эксплуатации системы. Таким образом, параметры помехоустойчивого кода выбирают исходя из некоторого «среднего» состояния канала связи, что приводит к уменьшению скорости передачи информации, из-за большей избыточности кода. Это может приводить к потере связи при использовании кодов, параметры которых остаются постоянными и не рассчитаны на значительное ухудшение качества канала. Одним из путей устранения этого недостатка является использование систем адаптивного кодирования с автоматической и целенаправленной коррекцией параметров кода по мере изменения качества канала, обеспечивая при этом заданную вероятность доведения сообщения при минимальной избыточности помехоустойчивого кода.

Одним из известных методов адаптивной передачи является адаптивная модуляция, которая заключается в поддержании постоянного отношения сигнал/шум путем подстройки мощности передатчика, скорости передачи, методов модуляции и кодирования [1]. Это позволяет обеспечить заданную вероятность ошибки, передавая данные с большей скоростью тогда, когда канал находится в хорошем состоянии, и снижая скорость при его ухудшении. В настоящее время формы адаптивной модуляции воплощены в некоторых приложениях радиосвязи, таких как подсистема HSDPA стандарта W-CDMA (до 16-КАМ); IEEE 802.11, IEEE 802.16 (до 64-КАМ) [1]. Однако существенным сдерживаемым фактором использования адаптивной модуляции, например, в мобильных каналах связи является изменяющиеся во времени параметры каналов, а также временная задержка управляющей информации в каналах обратной связи.

Другой метод адаптивной передачи, используемый в многочастотных системах, представляют собой адаптивную турбо-кодированную модуляцию, используемую в системах с ортогональным частотным разделением каналов (OFDM). Смежные подканалы

группируются в полосы, в пределах которых используется одна схема кодированной модуляции, выбираемая в расчете на наихудший подканал. Простейший из методов адаптивной передачи с использованием кодового разделения описан в [2]. Суть метода состоит в том, что данные каждого пользователя передаются только по одному наилучшему подканалу. Т.е. предпринимается попытка найти такую пару пользователей, входящих в две различные группы, обмен которыми приводит к увеличению текущей пропускной способности системы. Это позволяет снизить мощность передатчика, требуемую для достижения некоторой вероятности ошибки.

Известен также способ передачи информации по протоколу Международного Союза электросвязи ITU-TV.42, предусматривающий исправление ошибок в процедуре адаптивной сборки пакетов информации, при котором передают пакеты информации различной длины, защищенные помехоустойчивыми кодами. Пакет может содержать 32, 64, 128, 192 или 256 байт информации. При ухудшении состояния канала, информацию передают меньшими пакетами, а при улучшении качества канала, данные передаются пакетами больших размеров. В результате повышается вероятность правильного приема сообщения [3]. Недостатком этого способа является снижение достоверности принимаемой информации, так как декодирование помехоустойчивого кода осуществляется только с обнаружением ошибок. При этом не выдерживается оптимальное соотношение между количеством исправляемых и обнаруживаемых ошибок, которое соответствует состоянию канала связи в текущий момент времени.

Также распространен способ передачи информации с использованием помехоустойчивого адаптивного кодирования, в соответствии с которым на передающей стороне осуществляют непрерывный контроль за состоянием канала связи (за уровнем шумов, помехи и т.д.). Результаты контроля качества канала связи используются для выбора помехоустойчивых наилучших кодов, при этом используются две схемы кодирования: первая из них осуществляет кодирование информации с помощью циклического помехоустойчивого кода с обнаружением ошибок, а вторая − с помощью кода с исправлением ошибок. Далее выбранный помехоустойчивый код передают в канал связи. На приемной стороне помехоустойчивый код декодируется с обнаружением или исправлением ошибок в зависимости от используемого кода [4]. Недостатком этого способа также является невысокая достоверность принимаемой информации, обусловленная тем, что решения о выборе помехоустойчивого кода и алгоритма его декодирования принимаются на передающей стороне канала связи.

Важным открытием для спутниковой связи стала разработка в 2003 − 2004 годах стандарта DVS-S2 для видеовещания, интерактивных услуг и других спутниковых приложений. В этом стандарте используется адаптивная модуляция и кодирования (ACM – Adaptive Coding & Modulation), которая оптимизирует параметры передачи для каждого пользователя в зависимости от условий передачи. Стандарт DVS-S2 предполагает использование следующей схемы кодирования: внутренний код с малой плотностью проверок на четность (Low Density Parity Check codes − LDPC) и внешнего кода Боуза-Чоудхри-Хоквингема (Bose-Chaudhuri-Hocquenghem - BCH). Эта схема предусматривает расширенное число коэффициентов кодирования (FEC 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 8/9, 9/10) при различных видах модуляции (QPSK, 8PSK, 16APSK, 32APSK) [5]. Технология адаптивного кодирования и модуляции позволяет динамически менять вид модуляции и коэффициент кодирования (эта пара называется модкодом) для каждого отдельного кадра прямого канала в зависимости от условий распространения сигнала при сохранении постоянной символьной скорости. Для применения LDPC-кода к действительной системе связи этот LDPC-код должен быть разработан так, чтобы подходить под запрошенную скорость передачи данных в системе связи. В частности, LDPC-коды с разными длинами кодовых слов необходимы для поддержки разных скоростей передачи данных согласно системным требованиям в адаптивных системах связи [6]. Тем не менее, LDPC-код используемый в системе DVS − S2, имеет только два типа длины кодового слова– 16200 и 64800, что ограничивает его применение, и каждый тип LDPC-кода использует независимую матрицу контроля четности.

Выделение нерешенных ранее частей общей проблемы. Формулирование целей статьи (постановка задачи)

В области унифицированных средств защиты информации существует необходимость в разработке универсальных систем защиты на основе методов адаптивного кодирования, которые допускают изменения характеристик системы передачи по двум измерениям: энергетический выигрыш за сет кодирования и скорость передачи, чтобы обеспечить оптимальное соотношение выигрыша/скорости при различных состояниях информационного канала. При адаптивном кодировании необходимо решить следующие основные задачи:

– определить качество состояния информационного канала связи;

– принять решение об изменении значений параметров кодера и декодера, для обеспечения

заданной вероятности доведения сообщения при минимальной избыточности кода.

– установить новые параметры кода в кодирующем и декодирующем устройстве.

В настоящее время известны итеративные методы коррекции параметров кода по результатам доведения сообщения, а более эффективная двухконтурная схема коррекции параметров кода в зависимости от качества канала связи практически не используется [7]. Также не достаточно исследованы методы определения качества канала связи по результатам декодирования кода и методы реализации помехоустойчивых кодов с переменными параметрами. Существенный прогресс в реализации систем с обратной связью может быть достигнут при использовании методов адаптивного кодирования. Использование последних позволит создать алгоритмическую основу для реализации универсальных устройств защиты от ошибок в составе унифицированного ряда оконечных устройств передачи данных. Это даст возможность, используя единое устройство защиты от ошибок обеспечить не только адаптацию к текущим изменениям статистики ошибок канала связи, но и удовлетворить широкому диапазону требований к достоверности передачи информации для различных видов связи.

Основными параметрами помехоустойчивого кода являются блоковая длина (блоковые коды) или длина кодового ограничения (свёрточные коды) и скорость кода, определяющие его избыточность и корректирующую способность [8]. Однако изменение параметров кода не всегда гарантирует необходимое минимальное кодовое расстояние, и помехоустойчивость может ухудшиться. Т.к. алгоритмы кодирования и декодирования некоторых кодов привязаны к структуре порождающих и проверочных полиномов кода, не все помехоустойчивые коды могут легко менять свои параметры.

В настоящее время к параметрам кода, которые могут быть использованы в качестве параметрической адаптации, следует отнести количество информационных и избыточных разрядов, приходящихся на кодовую комбинацию или список слов, подлежащих передаче. Существуют различные варианты коррекции параметров кода, основанные на удалении или добавлении проверочных, информационных символов (рис. 1). Первый вариант адаптивной коррекции кода, заключающийся в сокращении информационных разрядов, называется укорочением кода [9]. Такая процедура не приводит к повышению скорости кода, т.к.

$$R(i)=\frac{k-i}{n-i} \quad \text{при} \quad i=(0,\ f) \text{ и } n>k \tag{1}$$

есть функция монотонно убывающая. Подобный подход в системах обмена информацией полезен для решения задачи снижения сложности кодирующих и декодирующих устройств, при условии достижения требуемой исправляющей способности кода. Вторым вариантом коррекции параметров кода является техника перфорации или выкалывания проверочных разрядов. Перфорация линейных блоковых кодов состоит в удалении проверочных символов и это приводит к линейному блоковому коду с параметрами ($n-f$, k, d'), у которого минимальное расстояние $d' < d$. При этом скорость кода возрастает, т.к. число проверок уменьшается. Такая технология подобна удалению определенных столбцов из единичной матрицы проверок.

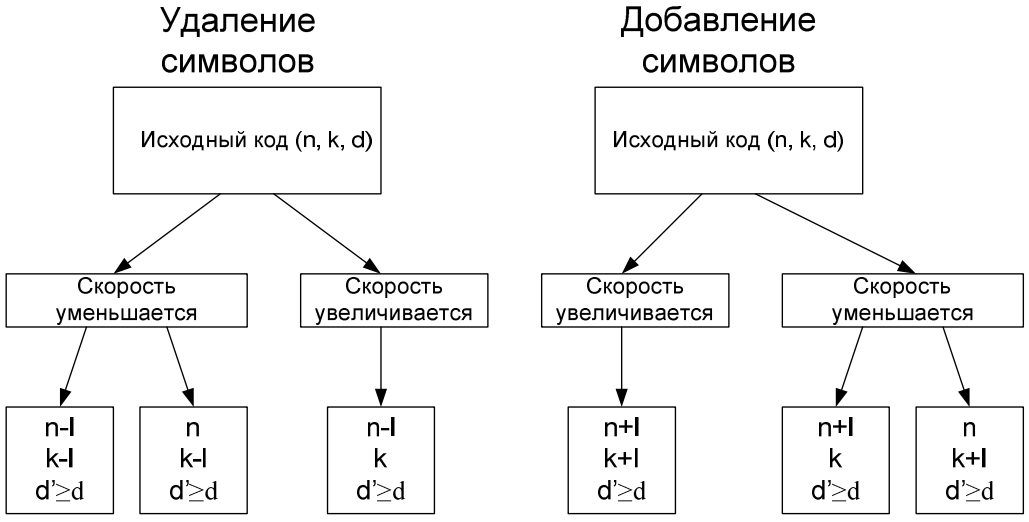

Рис. 1. Способы коррекции параметров помехоустойчивых кодов

Существуют совместимые по скорости, перфорированные сверточные коды (rate compatible punctured convolution codes – RCPC codes). Эти коды строятся из низкоскоростных кодов с помощью периодической перфорации, и за счет этого может быть повышена скорость кода. Например, если материнский код представляет собой сверточный код скорости 1/2, тогда матрицы перфорации $P(1)-P(4)$ порождают RCPC коды со скоростью 4/5, 4/6, 4/7, 4/8 соответственно. В адаптивных системах с автоматическим переспросом RCPC коды нашли свое применение, благодаря их способности к наращиванию избыточности, а также возможности построения кодов с переменной скоростью или кодов с неравной защитой [10].

Также существует способ расширения любого двоичного (n, k, d) кода до кода со значением $d_{min}= d + 1$, с помощью добавления к каждой кодовой комбинации результата суммирования по модулю 2 всех ее символов. Такое повторение кодовых комбинаций обеспечивает повышения минимального расстояния до двух, но при этом скорость кода снижается в два раза. Удлинение и пополнение кода заключается в увеличении числа информационных символов, которое влечет за собой увеличение размеров порождающей матрицы. Как правило, такие коды с коррекцией параметров, на приёмной стороне декодируются с помощью алгоритма списочного декодирования, который обеспечивает лучшее соотношение между сложностью и вероятностью ошибки, чем другие алгоритмы.

Для каналов со случайным характером ошибок практический интерес представляют лишь несколько кодов из десятка известных. Наиболее часто разработчики используют три вида кодов: свёрточные, Рида-Соломона и турбо коды, к которым относятся коды с низкой плотностью проверки на четность (Low Density Parity Check codes − LDPC) [11]. Сочетание нескольких схем помехоустойчивого кодирования позволяет учесть различные условия эксплуатации. Так свёрточный код обычно используется для передачи речевого трафика, когда вероятность ошибки на бит, может быть достаточно большой, но некритичной для восприятия и понимания передаваемой информации. При передаче данных, когда требуется более высокая надежность, применяются так называемые каскадные коды, в которых внешним обычно является код Рида-Соломона, а внутренний свёрточный. Для построения адаптивных систем кодирования среди помехоустойчивых кодов наибольший интерес представляют совместимые по скорости, перфорированные сверточные коды (Rate Compatible Punctured Convolutional Codes – RCPC) и гнездовые (вложенные) свёрточные коды (Nested Convolution Codes − NCC). Гнездовые свёрточные коды представляют собой набор кодов со скоростью $R = 1/(n+1)$, которые являются производными от сверточного кода скорости $R = 1/(n+1)$, с помощью поиска лучших генераторных последовательностей $G_{n+1}(D)$. Таким образом, используя технологию разложения материнского свёрточного кода на систему гнездовых (вложенных) свёрточных кодов, можно получить широкий набор кодовых соотношений (ЭВК), при этом сохраняя структуру и алгоритм кодирования материнского кодека. Синтез гнездовых свёрточных кодов, а также их свойства в настоящее время изучаются, также остается открытым вопрос о декодировании гнездовых свёрточных кодов. Однако представляет интерес построение адаптивной системы кодирования, на основе RCPC и NCC кодах, которая допускает изменения по двум измерениям: получение требуемой величины выигрыша за счет кодирования и обеспечение различных требований к информационной и канальной скорости.

Изложение основного материала исследования с полным обоснованием полученных научных результатов

Сигнально-кодовые конструкции для систем широкополосного доступа.

Все сигнально кодовые конструкции в соответствии с набором свойств делятся на группы, в соответствии с решаемой функциональной задачей. При создании нового поколения СКК одним из требований является унификация по используемым видам модуляции в части ширины спектра радиоизлучения с находящимися в эксплуатации системами. Детальная проработка требований к современным системам радиосвязи позволила сформировать четыре основные группы сигнально-кодовых конструкций.

– СКК, используемые для автоматического установления и ведения соединения. Характеризуются высокой устойчивостью к шумовым, структурным, импульсным и узкополосным помехам, многолучевому распространению, допплеровскому размытию и сдвигу частот в канале. Эта группа основана на шумоподобном сигнале, формируемом как разделимый код с максимальным расстоянием.

– СКК, используемые для среднескоростной передачи данных. Благодаря сверхбольшому канальному алфавиту сигнально-кодовой конструкции, 224 и более различаемых канальных символов, скорость передачи 2400 бит/с обеспечивается при длительности канального символа 20 мс, что позволяет работать в условиях сильной многолучёвости. Разработанные модификации также обеспечивают работу в условиях узкополосных и импульсных помех в полосе сигнала [12].

– СКК высокоскоростной (более 2400 бит/с) передачи данных. В настоящее время проводятся

работы по новому поколению этих сигналов, обладающему более низким пикфактором по сравнению с сигналами параллельных (OFDM) модемов. Также перспективные сигналы не будут нуждаться в затратных процедурах коррекции импульсной характеристики канала, занимающих в модемах последовательного типа по стандарту MIL-STD-188-110B до 25 % пропускной способности канала.

− СКК типа CHESS (Correlated Hopping Enhanced Spread Spectrum), использующие расширение спектра сигнала коррелированными скачками по частоте. Эта группа сигналов предназначена для передачи небольших объёмов информации. При скорости псевдослучайной перестройки по частоте до 200 скачков в секунду в полосе до десятков мегагерц, сигналы этого типа обладают высокой скрытностью и устойчивостью как к обнаружению, перехвату, так и к любым видам естественных и искусственных помех [13].

Зависимость энергетической эффективности от удельной скорости для различных систем широкополосного доступа представлены на рис. 2, связывая помехоустойчивость с пропускной способностью.

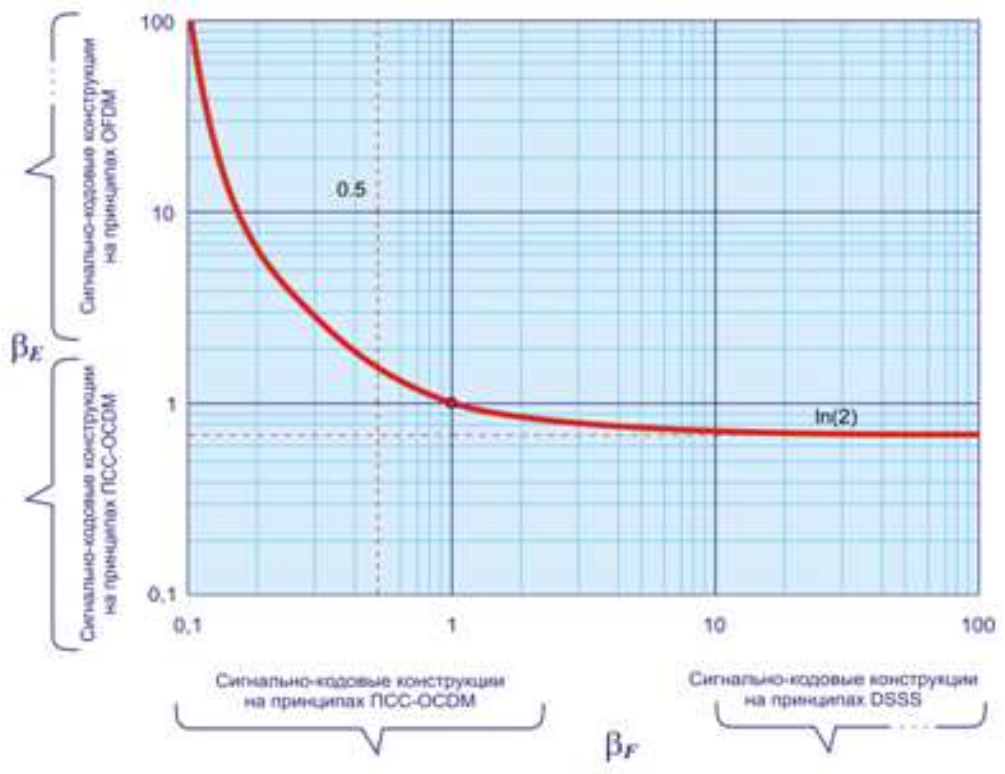

Рис. 2. Зависимость энергетической эффективности от удельной скорости

Из графика следует, что в зависимости от цели использования системы связи можно отметить 3 основных направления построения сигнально-кодовых конструкций [14]:

− сигнально-кодовые конструкции на основе OFDM сигналов для систем связи, обеспечивающих максимальную пропускную способность для заданных полос пропускания и вероятности ошибки в условиях естественных помех;

− сигнально-кодовые конструкции на основе CDM сигналов с прямым расширением спектра (DSSS) для систем связи с максимальной помехоустойчивостью в условиях воздействия любых помех;

− сигнально-кодовые конструкции для систем связи с максимально возможными помехоустойчивостью и пропускной способностью в условиях внутрисистемных и внешних помех, получившие название ортогонально-кодовое разделение каналов (OCDM).

Существенным недостатком при использовании таких типов СКК в общей полосе частот является спектральное проникновение сигналов, что влечет за собой увеличение удельных затрат полосы

пропускания. Помехозащищенность трех рассмотренных технологий построения систем широкополосного доступа может быть существенно повышена путем реализации сигнально-кодовых конструкций, на основе сигналов с искусственно создаваемым широкополосным спектром.

Оценка качества канала связи в системах передачи информации

Одним из методов контроля каналов передачи данных является контроль по вторичным статистическим характеристикам – статистике ошибок в последовательности дискретных элементов и блоках информации с учетом зависимого характера их искажения. Для оценки неизвестной вероятности используется, как правило, коэффициент ошибок по единичным элементам (кодовым комбинациям). Однако его применение целесообразно лишь на каналах с распределением ошибок, близким к независимому. Оценка состояния каналов, характеризующихся группированием ошибок элементов (что приводит к взаимосвязи искажений предаваемых блоков информации) при использовании указного метода становится явно неадекватной и ведет к значительным ошибкам контроля. Поэтому применимость этого метода ограничивается периодом квазистационарности состояния канала связи.

Известен способ контроля качества канала связи, при котором осуществляют передачу испытательной последовательности по каналу связи. На выходе канала из принятой испытательной последовательности вычитают передаваемую испытательную последовательность, и в результате получают последовательность ошибок, а затем вычисляют параметры канала связи, характеризующие его качество. Недостатком этого способа является снижение скорости передачи полезной информации, обусловленное тем, что определение качества канала связи осуществляют при передаче по каналу испытательной последовательности, и канал в это время предоставлен для проведения измерений.

В [11-14] предложен способ контроля качества канала связи, по результатам которого выбирают помехоустойчивый код с переменными параметрами. Контроль качества канала связи осуществляют на приемной стороне по результатам декодирования слов внутреннего помехоустойчивого каскадного кода. При этом характеристики канала связи описывают двумя параметрами: средней вероятностью ошибки на бит и коэффициентом группирования ошибок по модифицированной модели канала связи Пуртова. Недостатком этого способа является низкая достоверность контроля, поскольку в каналах низкого качества событие неискаженного приема слов помехоустойчивого кода может происходить с небольшой вероятностью. Также достоверность контроля снижается из-за того, что на приёмной стороне неизвестно количество переданных слов помехоустойчивого кода.

При аналитическом исследовании или статистическом испытании дискретных каналов очень широко используются вероятностные характеристики потока ошибок на выходе информационного канала. Обычно в качестве таких характеристик используются:

– усредненная вероятность появления ошибки p_σ на множестве исходных символов ДКС;

– вероятность искажения кодовой последовательности $P(i(1,n))$ на множестве кодовых последовательностей на выходе информационного канала;

– функция кратности ошибок $P(m,n)$, которая определяется как вероятность появления m ошибок на кодовой последовательности длины n.

Знание этих характеристик, с одной стороны, позволяет определить свойства реальных каналов связи и разработать на их основе математические (имитационные) модели, алгоритмы которых описывают с достаточной степенью точности отзыв среды распространения на форму и вид сигналов, которые передаются. С другой стороны, эти характеристики дают возможность оценить вероятности ошибочного декодирования при использовании кодов с заданным кодовым расстоянием в режиме исправления ошибок по минимальному Хэминговому расстоянию, не проводя сложных процедур кодирования и декодирования.

В зависимости от помеховой обстановки в канале передачи дискретной информации возможны следующие различные задачи, связанные с проблемами выбора параметров и построения, на их основе корректирующих кодов:

– построение кода с максимальным значением $d_{\min}$ при заданных n и v;

– построение кода с максимальным значением v при заданных n и $d_{\min}$;

– построение кода с максимальным значением n при заданных v и $d_{\min}$;

Как следует из перечисленных задач, из тройки параметров кода, два из них априори должны быть заданы. Это обстоятельство является существенным ограничением при выборе кода, оптимального к статистике ошибок в реальных каналах связи. Выполненная ранее оценка потенциальных границ для вероятности ошибки декодирования позволяет снять указанное ограничение и увязать топологические характеристики разбиения последовательности ошибок на блоки с параметрами кодов. При этом длина n-последовательности ошибок $e_{[n]}(d)$ адекватна длине

кодового блока n, а m ($m \geq d$) является весовой функцией ошибки на $e_{[n]}(d)$, минимизирующей значение потенциальной вероятности ошибки декодирования на множестве (n, m) - разбиений последовательности ошибок и связанной с минимальным кодовым расстоянием соотношением

Для корректирующих кодов верхняя граница Хэмминга [11]

$$R \leq 1 - \frac{log_2 \sum_{j=1}^{d_g - 1} C_{n-1}^{j}}{n}. \qquad (2)$$

Таким образом, представляется возможным определить параметры корректирующих кодов, адекватные топологическим характеристикам (n, m) − разбиений последовательности ошибок $E(\nu)$ на выходе дискретного канала и оптимальные к ее статистическим характеристикам. В то же время по результатам имитационного моделирования показано, что условие (2) выполняется для некоторого множества $\{n_j\}$ $j = \overline{1...\xi}$ значений длин разбиений при фиксированной весовой функции $m(d)$ последовательностей ошибок $e_{[n]}(d)$. С учетом этого свойства выражение (2) может быть записано в виде системы равенств

$$\nu \geq n - log_2 \sum_{j=1}^{d_g - 1} C_{n-1}^{j}. \qquad (3)$$

Выражение (3) является «краеугольным камнем» в определении параметров кода, адаптируемого к состоянию канала связи, поскольку позволяет изменять (перфорировать) длину кодового блока n, изменяя тем самым корректирующие свойства кода в зависимости от изменения статистики ошибок в канале связи.

Выводы

В комплексе проблем разработки и создания единой автоматизированной системы управления важное место принадлежит реализации высокоэффективных унифицированных аппаратно-программных модулей защиты и передачи информации. Возрастающие требования к достоверности и своевременности передачи информации в специализированных компьютерных системах в сочетании с жесткими требованиями к вероятностно-временным характеристикам доведения сообщения требует усовершенствования и разработки универсальных средств защиты и передачи информации.

Проведенный анализ работ в области проектирования аппаратно-программного обеспечения для передачи информации в компьютеризированных интегрированных системах показал, что отсутствует единый методологический подход, ориентированный на создание универсальных модулей защиты информации, позволяющих обеспечить оптимальное соотношение энергетического выигрыша и скорости передачи. Основным недостатком информационных систем передачи данных в автоматизированных системах связи – каждое устройство защиты от ошибок разрабатывается под каждый тип канала связи и конкретный вид связи, что порождает большое количество разнообразных устройств, которые реализуют одну и ту же функцию – защита информации от ошибок. Также существующие способы защиты информации от ошибок не учитывают топологию потока ошибок на выходе реальных каналов связи. Таким образом, целью диссертационной работы является повышения достоверности и скорости передачи информационных сообщений в компьютеризированных интегрированных системах, на основе разработки и усовершенствовании унифицированных методов и алгоритмов защиты и передачи информации, реализуемых на современной элементной базе.

Литература

1. Крылова В.А. Оценка возможности унификации методов передачи данных в сетях связи с интеграцией служб / В.А. Крылова, В.В. Горбачев // Вісник НТУ «ХПІ». – Харків : НТУ «ХПІ», 2005. − №7 – С. 36−40.
2. Крылова В.А. Методы адаптивного кодирования для каналов с переменными параметрами / В.А. Крылова, В.В. Горбачев, С.Ю. Гавриленко // Вісник НТУ «ХПІ». – Харків : НТУ «ХПІ», 2008. − №31 – С.19−26.
3. Крылова В.А. Оценка возможности построения универсальных кодеков на основе свёрточных кодов с алгоритмом декодирования Витерби / В.А. Крылова, В.В. Горбачев // Вісник НТУ «ХПІ». – Харків : НТУ «ХПІ», 2008. − №57 – С. 44−52.
4. Крылова В.А. Гибкий алгоритм Витерби для декодирования свёрточных кодов с переменными параметрами / В.А. Крылова, В.В. Горбачов // Вісник НТУ «ХПІ». – Харків : НТУ «ХПІ», 2010 г. − №20 – С. 45−51.
5. Крылова В.А. Метод синтеза гнездовых свёрточных кодов с переменными параметрами / В.А. Крылова // Вісник НТУ «ХПІ». – Харків : НТУ «ХПІ», 2011. − №11 − С. 80−86.
6. Крылова В.А. Методика выбора параметров гнездовых свёрточных кодов / В.А. Крылова // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків : НТУ «ХПІ», 2011. − №57 – С. 74−78.

7. Крылова В.А. Оценка информационного состояния канала связи в адаптивных системах кодирования/декодирования / В.А. Крылова // Вісник НТУ «ХПІ». – Харків : НТУ «ХПІ», 2013. − №8(982) – С. 64−70.
8. Крылова В.А. Гнездовые свёрточные коды с переменной параметрами в адаптивных системах кодирования / В.А. Крылова // Вестник Казахской академии транспорта и коммуникаций им. М. Тынышпаева – Алмата: КазАТК, 2013. − №5(84) – С.77−83.
9. Miroshnik M.A. Uses of programmable logic integrated circuits for implementations of data encryption standard and its experimental linear cryptanalysis / M.A. Miroshnik, M.A. Kovalenko // Інформаційно – керуючі системи на залізничному транспорті. – – 2013. – №6,с.36-45.
10. Крылова В.А. Реализация адаптивного устройства кодирования/декодирования на ПЛИС / В.А. Крылова // Вісник НТУ «ХПІ». – Харків : НТУ «ХПІ», 2014. − №15 (1058) – С. 86−90.
11. Крылова В.А. Сигнально-кодовые конструкции для адаптивных методов кодирования в многоканальных системах связи / В.А. Крылова, В.В. Горбачов // Інформаційно-керуючи системи на залізничному транспорті. – Харків : УкрГАЖТ, 2014. − №1(104) – С. 56−58.
12. Мирошник М.А. Методы защиты цифровой информации в распределенных компьютерных сетях / М.А. Мирошник // Інформаційно – керуючі системи на залізничному транспорті. – 2014. – №5, с.66-70.
13. Мирошник М.А. Разработка систем защиты информации распределенных автоматизированных систем управления / М.А.Мирошник // Систем и обробки інформації. – 2013 – №7 (114), с.86-89.
14. Мирошник М.А. Разработка средств защиты информации от в распределенных компьютерных системах и сетях / М.А. Мирошник // Інформаційно-керуючі системи на залізничному транспорті. – 2015. – №1, с.18-25.

Крилова В.А., Мірошник А.М. Розробка методів оцінки ефективності систем захисту інформації в розподілених комп'ютерних системах. Стаття присвячена розробці та удосконаленню методів, засобів захисту, обробки і передачі інформації, оцінки ефективності систем захисту інформації в розподілених інформаційних системах спеціального призначення. Запропоновано рішення задачі оперативного знаходження параметрів завадостійкого коду. Розроблено метод визначення якості каналу зв'язку на основі оцінки статистичних характеристик потоку помилок.

У статті запропонована технологія синтезу сигнально-кодових конструкцій на основі системи сигналів з гребінчастим спектром і адаптивним кодуванням. Запропоновано алгоритм знаходження коефіцієнтів цифрових фільтрів для реалізації системи ущільнення сигналів методами умовної мінімізації перехідних перешкод між поєднуваними сигналами.
Ключові слова: комп'ютеризовані системи та мережі, система захисту інформації, адаптивне кодування, широкосмугові сигнали, сигнально-кодові конструкції, гребінчастий фільтр.

Krulova V.A., Miroshnik A.N. Development of methods for evaluating the effectiveness of information security systems in distributed computer systems. Article is devoted to the development and improvement of methods, protection, processing and transmitting information, evaluate the effectiveness of information security systems in distributed information systems for special applications. Provides a solution to the problem of finding the operational parameters of error-correcting code. A method for determining the quality of the communication channel based on the assessment of the statistical characteristics of the flow errors.

The paper proposes a synthesis technology of signal-code constructions based on a system of signals with a comb spectrum and adaptive coding. An algorithm for finding the coefficients of digital filters for the implementation of the sealing system signals methods for constrained minimization of crosstalk between the combining signals.
Key words: computerized system and network information security system, adaptive coding wideband signals, signal-code construction, comb filter.

Рецензент д.т.н., профессор, профессор кафедры АУТС Качанов П.А. (НТУ «ХПИ»)

Поступила 23.03.2015г.