Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

3. Железняк В.К. Защита информации от утечки по техническим каналам: учеб. пособие. СПб.: ГУАП, 2006. 188 с.

4. Кошевая Л.А. Обеспечение единства испытаний. Концептуальные основы. – К.: НАУ-друк, 2009. 176 с.

5. Расчет транзисторных цепей / под ред. Р.Ф. Ши. – М.: Энергия, 1964. 204 с.

6. Корни Ш. Теория цепей. Анализ и синтез. М.: Связь, 1973. 308 с.

7. Марпл-мл. С.Л. Цифровой спектральный анализ и его приложения. – М.: Мир, 1990. 584 с.

8. Шатихин Л.Г. Структурные матрицы и их применение для исследования систем. – М.: Машиностроение, 1974. 248 с.

9. Липницкий В.А. Высшая математика. Основы линейной алгебры и аналитической геометрии : уч. пособие для курсантов учреждений высшего образования. – Минск: ВА РБ. 2015. 229 с.

10. Демидович Б.П., Марон П.А. Основы вычислительной математики : учеб. пособие для студ. высш. техн. учеб. заведений. – М.: Наука, 1970. 664 с.

АНАЛИЗ ЭФФЕКТИВНОСТИ И ПОМЕХОЗАЩИЩЕННОСТИ МНОГОКАНАЛЬНЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ С КОДОВЫМ УПЛОТНЕНИЕМ

В.О. СИДОРОВИЧ, А.Н. ГАВРИЧЕНКО, А.Е. ВАРЮШИНА

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»

Введение

Практика построения современных СПИ показывает, что наиболее дорогостоящими звеньями трактов передачи являются линии связи (кабельные, волоконно-оптические, сотовой мобильной радиосвязи, радиорелейной и спутниковой связи и т. д.). Поскольку экономически нецелесообразно использовать дорогостоящую линию связи для передачи информации единственной паре абонентов, то возникает необходимость построения многоканальных СПИ, обеспечивающих передачу большого числа сообщений различных источников информации по общей линии связи [1].

В многоканальной СПИ по общему высоко-частотному тракту передаются сообщения от нескольких источников информации. На передающей стороне многоканальной системы сообщения от каждого из источников информации модулируют по какому-либо параметру выделенные данному источнику канальные сигналы. Затем промодулированные канальные сигналы объединяются по тому или иному правилу, в результате чего формируется суммарный (групповой) сигнал. Данная операция называется *уплотнением каналов*. Полученный групповой сигнал затем модулирует несущее колебание, которое поступает на передачу. При использовании общей несущей канальные сигналы иногда называют *поднесущими* колебаниями. В ряде случаев, когда источники информации территориально сосредоточены, общая несущая не используется и канальные сигналы формируются непосредственно на несущих частотах. На приемной стороне многоканальной радиолинии после демодуляции несущей осуществляется операция, обратная операции уплотнения – из группового сигнала выделяются сигналы отдельных каналов. Данная операция называется *разделением (селекцией) каналов* [2].

1. Многоканальные радиосистемы передачи информации с кодовым линейным уплотнением

Тракт связи по способности передавать информацию характеризуется объемом V_{MP}:

$$V_{MP} = F_{MP} \cdot T_{MP} \cdot Д_{MP},$$

где F_{MP} — полоса частот тракта связи,

T_{MP} — время использования тракта связи,

$Д_{MP}$ — динамический диапазон тракта связи.

Передаваемый по тракту связи сигнал также имеет три измерения, т. е. тоже имеет объем $V_C = F_C \cdot T_C \cdot Д_C$.

Для передачи сигнала по тракту связи с допустимыми искажениями необходимо выполнить условие, чтобы $V_{MP} \geq V_C$.

Возможные методы уплотнения каналов можно классифицировать на линейные и нелинейные. К линейным относятся такие, при которых уплотнение сигналов отдельных каналов производится линейными устройствами с постоянными или переменными параметрами. В противном случае методы уплотнения являются нелинейными[3].

Если объем тракта связи намного больше объема передаваемого сигнала, то возможно уплотнение тракта связи n каналами передачи информации. В зависимости от того, какой из параметров тракта связи делится по отдельным каналам, различают методы: частотного и временного уплотнения, а также уплотнения по уровню (кодовое). Указанные методы уплотнения тракта связи являются линейными [2].

При использовании линейных методов операция уплотнения каналов сводится к суммированию канальных сигналов. В кодовом линейном уплотнении в качестве ансамбля канальных сигналов используются ортогональные системы тригонометрических функций, функций Радемахера-Уолша, полиномы Лежандра, Чебышева и др. Групповой сигнал представляется в виде суммы ортогональных канальных сигналов. Разделение сигналов на приемной стороне осуществляется n линейными избирательными устройствами (по числу каналов), каждое из которых выделяет соответствующий канальный сигнал из группового. Для линейного разделения каналов при линейном уплотнении необходимым и достаточным условием является линейная независимость канальных сигналов, при которой ни один из них нельзя представить линейной комбинацией других канальных сигналов[3].

2. Многоканальные радиосистемы передачи информации с кодовым нелинейным уплотнением (комбинационное уплотнение)

Общая теория нелинейного уплотнения и разделения каналов к настоящему времени еще достаточно не разработана. Поэтому ограничимся рассмотрением так называемого комбинационного метода, который является одним из примеров нелинейного уплотнения и разделения каналов.

Пусть имеется L_U каналов, в которых сообщения, подлежащие передаче, представлены в цифровой форме, например, двоичным кодом. Символы кода «0» и «1» из всех каналов одновременно поступают на устройство уплотнения. Поскольку в каждом из каналов возможно появление как «0», так и «1», то, очевидно, в любой фиксированный момент времени на устройство уплотнения от всех L_U каналов поступает одна из 2^{L_U} возможных комбинаций «0» и «1». В общем случае, при представлении сообщения в каждом из каналов с помощью кода с основанием b (6-ичного кода, где $b \geq 2$), в любой

фиксированный момент времени на устройство уплотнения от всех L_U каналов будет поступать одна из b^U возможных комбинаций символов 0, 1, ... , $b-1$. Устройство уплотнения каждой из поступивших комбинаций ставит в соответствие свой номер (однозначно соответствующее этой комбинации число), который и является групповым сигналом. Таким образом, при данном методе уплотнения групповой сигнал не является линейной комбинацией канальных сигналов, а представляет собой однозначное отображение возможных комбинаций канальных символов, чем и объясняется название данного метода уплотнения. Групповой сигнал может кодироваться различными способами. На приемной стороне по принятому групповому сигналу восстанавливаются символы кодов сообщений в каждом из каналов, т. е. осуществляется разделение каналов. Данное разделение возможно, потому что любая комбинация символов кода сообщения однозначно соответствует групповому сигналу. В общем случае разделение каналов осуществляется нелинейными устройствами, хотя возможны модификации комбинационного уплотнения, при которых разделение осуществляется линейными устройствами[4].

3. Многоканальные радиосистемы передачи информации с кодовым нелинейным уплотнением (мажоритарное уплотнение)

На выбор того или иного типа кода группового сигнала существенное влияние оказывает сложность реализации соответствующей операции нелинейного преобразования (операции уплотнения) и обратной операции (операции разделения каналов). В этой связи большой интерес представляет один из частных случаев комбинационного уплотнения – логическое или мажоритарное уплотнение каналов. В результате данного уплотнения каждой комбинации двоичного кода с блоковой длиной $П_C$ в параллельной форме поступившей от уплотняемых источников, в устройстве уплотнения ставится в однозначное соответствие комбинация двоичного кода группового сигнала с блоковой длиной $П$, представленного в последовательной форме. При этом значение каждого двоичного символа кодовой комбинации группового сигнала определяется в соответствии с логической функцией абсолютного большинства, т. е. мажоритарно, что и определяет название данного метода уплотнения.

Двоичный код группового сигнала, получаемый при мажоритарном уплотнении, удобен для дальнейших преобразований на передающем стороне и обработки на приемной стороне и имеет минимально возможный пикфактор, что позволяет полностью использовать потенциальные возможности радиопередающего устройства. При этом нелинейность группового тракта не приводит к появлению междуканальных помех. Кроме того, при данном методе уплотнения оказывается возможным линейное разделение каналов, просто реализуемое полностью цифровым устройством разделения [5].

Заключение

На сегодняшний день важнейшими достоинствами кодового уплотнения являются эффективное использование выделенной полосы частот (все каналы занимают одну и ту же полосу частот в одном временном интервале), обеспечивается высокая потенциальная помехоустойчивость (за счет ортогональных функций) и высокая помехозащищенность, возможность обеспечить энергетическую и структурную скрытности передаваемой информации.

Список литературы

1. Принципы многоканальной передачи информации. Элементы теории разделения сигналов [Электронный ресурс]. – 2011. – Режим доступа : http://studopedia.org/8-106652.html – Дата доступа: 26.01.2015.

2. Уплотнение информации в аналоговых системах связи [Электронный ресурс]. – 2014. – Режим доступа: http://studopedia.org/2-74270.html – Дата доступа: 11.03.2014.

3. Садомовский, А.С. Приемно-передающие радиоустройства и системы связи / А.С. Садомовский // Ульяновск: УлГТУ, 2007. – 243 с.

4. Тепляков, И.М. Радиолинии космических систем передачи информации / И.М. Тепляков, И.Д. Калашников, Б.В. Рощин // М.: Сов. радио, 1975. – 400 с.

5 Общие положения и классификация методов уплотнения каналов [Электронный ресурс]. – 2011. – Режим доступа: http://www.studfiles.ru/preview/4287735/page:6/ – Дата доступа: 31.05.2015.

О РАЗВИТИИ СРЕДСТВ ДОВЕРЕННОЙ ЗАГРУЗКИ

Д.Ю. СЧАСТНЫЙ

Закрытое акционерное общество «ОКБ САПР»

Средства доверенной загрузки (далее по тексту СДЗ) за последние несколько лет получили существенное развитие. Причин тому видится две: формализация требований к СДЗ со стороны регулятора (ФСТЭК России) и отказ от средств вычислительной техники на базе архитектуры x86 в Государственных Информационных Системах (ГИС) в пользу «альтернативных» архитектур.

Напомню, что с 1 января 2014 года сертификация средств защиты информации, реализующих функции доверенной загрузки, в системе сертификации ФСТЭК России проводится на соответствие Требованиям к средствам доверенной загрузки, утвержденным приказом ФСТЭК России от 27 сентября 2013 г. № 119 [1]. Кроме того, регулятор обязывает применять только сертифицированные средства при построении ГИС и обработке персональных данных [2–3]. Таким образом, разработчики СДЗ получили некоторый формальный набор требований, соответствуя которому, могут называть свой продукт СДЗ. А Заказчики легально применять этот продукт, опираясь на формальное соответствие необходимому классу.

Вторым важным двигателем процесса развития СДЗ видится переход на «альтернативные» архитектуре x86 архитектуры СВТ в ГИС. Такой переход набирает обороты, все чаще в СМИ упоминаются реализованные проекты ГИС, построенные на Эльбрусах, Байкалах или «новой гарвардской архитектуре» [4]. По причине молодости этого рынка СДЗ для них пока очень мало, но создавать их, конечно, необходимо. Причем помимо требований Регулятора, о которых речь шла выше, все-таки основным моментом, мотивирующим Заказчиков ГИС применять СДЗ, должно быть основное предназначение СДЗ – обеспечение доверенной загрузки. При общении с разработчиками и Заказчиками подобных систем можно часто услышать мнение, что применение СДЗ у них необязательно, так как «процессор доверенный, закладок не содержит, враг не пройдет». Но даже самый проверенный процессор с не менее проверенным БИОСом, не содержащим закладок, не выполняет контроль целостности файлов и данных ДО старта операционной системы (ОС). И не производит идентификацию/аутентификацию пользователей ДО старта ОС. И в целом не гарантирует доверенную загрузку ОС. У него другая задача. И именно по этой причине СДЗ нужно применять и на проверенных и доверенных процессорах тоже.

В соответствии в вышеописанными тенденциями можно выделить несколько направлений, по которым идет развитие СДЗ. Во-первых, продолжается развитие традиционных аппаратных СДЗ вслед за развитием средств вычислительной техники