ПРИНЦИПЫ ПОСТРОЕНИЯ СОВРЕМЕННЫХ ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ С ЗАЩИЩЕННЫМИ КАНАЛАМИ СВЯЗИ

Цопа А.И.
Научный руководитель: д-р техн. наук, проф. Шокало В.М.
Харьковский национальный университет радиоэлектроники,
Кафедра основ радиотехники
пр. Ленина, 14, г. Харьков, 61166, Украина
Тел.: +38 057 702 15 87; e-mail: knure-res@kharkov.ukrtel.net

Abstract — The new principles of development of digital information transmission system with communication channel protection on energy level are proposed in article.

1. Введение

Современный этап развития цифровых систем передачи информации (ЦСПИ) связан с технологическим прорывом в области микро- и наноэлектроники.

Появление новой производительной элементной базы, позволяющей реализовывать ЦСПИ в физически малых объемах, привело к глобальной интеграции различных технологий, как по назначению, так и по принципу действия.

Наряду с требованиями высокой производительности системы связи, одним из основных требований предъявляемым к современным ЦСПИ является обеспечение защищенности каналов связи. В этой направлении идет бурное развитие как информационных, так и технических методов защиты информации. Это развитие должно привести к интеграции и в сфере технологий защиты информации (ЗИ), находящихся на различных ступенях семиуровневой модели взаимодействия открытых систем (*OSI*).

При этом очевидно, что в связи с массовым внедрением цифровых технологий передачи информации обеспечить повышенные требования безопасности только одними информационными (криптографическими) методами не представляется возможным. В этих условиях необходимо искать новые пути повышения защищенности каналов связи не только на информационном, но и на физическом (энергетическом) уровне.

В докладе основное внимание уделено определению круга нерешенных задач по защите информации на энергетическом уровне.

2. Основная часть

Одним из мощных направлений развития ЦСПИ является интеграция проводных и беспроводных технологий.

В настоящее время основными цифровыми технологиями передачи информации по проводным каналам связи являются различные широкополосные *xDSL* технологии, обеспечивающие высокую скорость передачи информации по существующим кабельным линиям связи (КЛС).

В сегменте беспроводных технологий абонентского доступа ведущие позиции занимают технологии *Wi-Fi*, на которых строятся ЦСПИ для локальных сетей (*WLAN*), и технологии *WiMAX*, на которых строятся ЦСПИ для городских сетей (*WPAN*). Эти технологии работают в диапазоне частот (2,4…5,2) ГГц и используют различные методы расширения спектра радиосигналов в канале связи.

В докладе рассмотрены некоторые примеры интеграции технологий и систем связи:

а) интеграция технологий использующих различные физические принципы для передачи информации: интеграция проводных и беспроводных сетей (например: *xDSL+WiMAX*, *xDSL+Wi-Fi)*; интеграция проводных и оптоволоконных сетей (*xDSL+FTT)* и т.п.;

б) интеграция беспроводных технологий разного радиуса действия: сетей персонального доступа (*WPAN*), сетей локального доступа (*WLAN*) и сетей городского масштаба (*WMAN*) (например: *Bluetooth+Wi-Fi+WiMAX)*;

в) интеграция систем передачи информации с системами извлечения информации и синхронизации (*WiMAX+GPS*, *Wi-Fi+GPS, Wi-Fi+WiMAX+GPS*).

Один из вариантов интеграции различных технологий и ЦСПИ при разворачивании информационной сети доступа в зоне кризисной или чрезвычайной ситуации (ЧС) показан на рис. 1 [1].

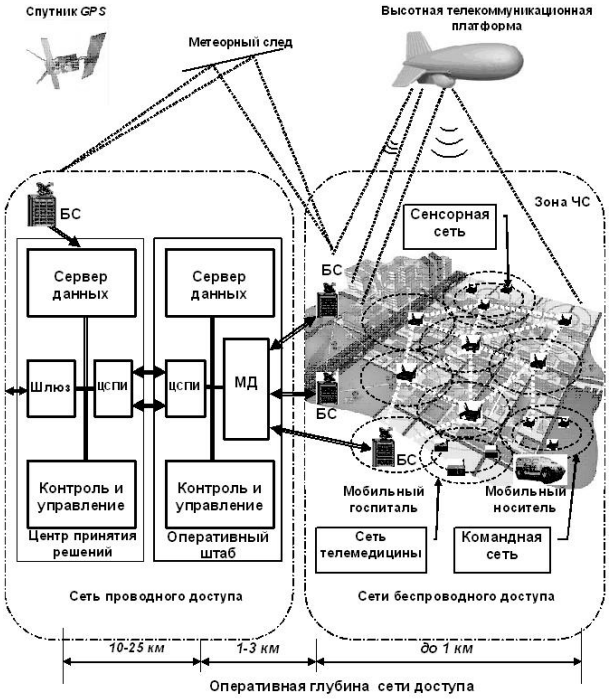

Рис. 1 — Структурная схема интегрированной сети доступа, разворачиваемой в зоне ЧС

Интегрированная сеть доступа включает в себя нескольких подсистем и сетей: сеть проводного доступа (СПД), сеть абонентского радиодоступа (САРД), сеть телемедицины, сенсорную распределенная радиосеть и командную радиосистему (КРС). Базовые станции (БС) системы радиодоступа подключаются по проводной сети к мультиплексору доступа (МД),

который обеспечивает концентрацию информационных потоков и подключение к серверу данных оперативного штаба. Для передачи информации на дальние расстояния в центр принятия решений используются проводные многоканальные ЦСПИ.

Также при организации связи в зоне ЧС в ряде случаев может понадобиться высотная телекоммуникационная платформа. Эта платформа представляет собой дирижабль, который устанавливается на высоте до (20…22) км, обеспечивая активную ретрансляцию радиосигналов и расширяя оперативную глубину зоны радиодоступа.

В значительно мере повысить надежность связи в зоне ЧС, особенно в труднодоступных районах, может также интеграция в ЦСПИ метеорного радиоканала (МРК). МРК возникает благодаря отражению метровых волн от ионизированных метеорных следов в атмосфере Земли. С его помощью можно передавать небольшие объёмы информации, в том числе и криптографические ключи, на большие расстояния (до 2000 км) при сравнительно небольшой средней мощности передающего устройства. Благодаря направленному характеру распространения отражённых от метеорных следов радиоволн заметно повышается энергетический потенциал линии связи и ограничивается возможность перехвата сообщений, передаваемых по метеорному каналу связи [2].

Обеспечение защищенности ЦСПИ, входящих в эту разветвленную ведомственную сеть связи (ВСС), является одной из основных задач, которые необходимо решать при разработке как отдельных элементов системы доступа, так и системы в целом. При этом под защищенностью системы связи понимается ее помехозащищенность и скрытность [3].

Основоположником информационного подхода при создании безопасных систем связи является К. Шеннон, положивший начало не только науки криптографии, но и науки кодирования канала связи. В своих работах он ввел понятие совершенной секретной системы связи и указал на способ построения не раскрываемого ключа [4].

Другой подход решения задачи повышения защищенности канала связи базируется на теории потенциальной помехоустойчивости, которая определяет предельную помехоустойчивость системы связи. Котельников В.А. предложил повышать помехоустойчивость системы связи на основе учета статистических свойств помех и статистического синтеза оптимальных приемников [5].

Первая попытка объединения этих двух подходов была предпринята в работах Зюко А.Г. В этих работах введены простые количественные показатели эффективности систем передачи информации, характеризующие степень использования основных ресурсов канала связи (информационная, энергетическая и частотная эффективность) [6].

Дальнейшим развитием теории построения защищенных систем связи является модель отводного канала связи, предложенная Вайнером А. В этой модели рассматривается ситуация, когда в канале связи имеется шум и вероятность ошибки в канале противника (отводном канале) выше, чем для основного канала, по которому легитимные абоненты обмениваются сообщениями [7].

При таком предположении возможно достижение совершенной стойкости криптосистемы с существенно меньшими требованиями к длине ключевой информации, чем в модели Шеннона. Кроме того, применение специальных систем кодирования позволяет вообще отказаться от криптографических методов защиты информации в канале связи [8].

На рис. 2 показана структурная схема модели канала связи с отводным каналом (каналом утечки).

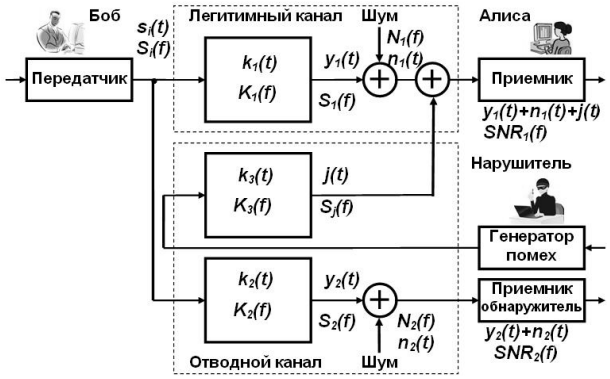

Рис. 2 — Структурная схема модели канала связи с отводным каналом

Для оценки защищенности такого канала связи целесообразно использовать такой параметр как секретная производительность C_S [7], который определяется как разность скорости передачи информации по Шеннону в легитимном канале связи C_1 и скорости передачи в отводном канале нарушителя C_2

$$C_s = \begin{cases} W\log_2(1+SNR_1) - W\log_2(1+SNR_2), \text{ при } SNR_1 > SNR_2 \\ 0, \text{ при } SNR_1 \le SNR_2 \end{cases}$$

Из этого выражения следует, что высокая защищенность канала связи $C_s = \max\left[C_s\right]$ может достигаться за счет увеличения скорости передачи информации в легитимном канале связи и повышения SNR_1 за счет знания параметров канала распространения по отношению SNR_2 в канале нарушителя ($SNR_1 >> SNR_2$).

Повышение скорости передачи информации в легитимном канале связи связано с использованием многоуровневых линейных кодов (*TC-PAM*) и дискретной мультитоновой модуляции (*DMT*) в проводных каналах связи и применением различных технологий расширения спектра *SS* (*Spread Spectrum*) в беспроводных каналах.

Наиболее распространенными технологиями расширения спектра сигналов являются:

— прямое расширение спектра (*DSSS*);

— скачкообразная перестройка частоты сигнала (*FHSS*);

— случайное время выхода в эфир (*THSS*);

— ортогональное частотное мультиплексирование (*OFDM*).

Основной особенностью этих технологий является использование псевдослучайных величин *PN* (*pseudo noise*) для установки уровня и кратности модуляции *M*, базы сигнала *B*, числа поднесущих частот f_n, времени *T* и последовательности выхода в эфир и др.

В качестве *PN* последовательностей применяются коды Баркера, *M*-последовательности, коды Уолша, алгебраические коды и другие, обладающие хорошими автокорреляционными свойствами.

Значительное увеличение длины (разрядности) этих последовательностей *PN* (более 1000) создает значительный массив вариантности структуры сиг-

нала в канале связи, что также может быть использовано для повышения защищенности канала связи на сигнальном уровне. Это обусловлено тем, что переборный механизм обработки в реальном масштабе времени таких сложных сигналов в канале перехвата будет сопряжен с большими аппаратными затратами и временем обработки.

Еще более существенным источником вариантности сигнальной структуры канала связи является применение *MIMO*-технологий *(Multi-Input Multi-Output)*, которые дополнительно вносят пространственную координату, создавая в канале связи многомерное пространство сигналов. Интеграция технологий расширения спектра сигналов и *MIMO*-технологий (*xDSL+MIMO*, *DSSS+MIMO*, *FHSS+MIMO*, *OFDM+MIMO* и т.п.) создает реальную основу построения защищенных ЦСПИ на физическом уровне.

Кроме многоуровневых методов модуляции сигнала и пространственного размещения приемопередающих антенн важной особенностью современных технологий связи является наличие развитых механизмов адаптации к каналу связи. Эти механизмы дают возможность не только повысить производительность системы, но и улучшить качество передачи информации на канальном уровне (за счет применения различных методов коррекции ошибок). Отсутствие у противника полной информации о параметрах, механизмах адаптации и коррекции ошибок не даст ему возможность получать достоверную информацию на сигнальном уровне, а значит и возможности информационного вскрытия канала связи будут значительно уменьшены.

Для аппаратной реализации защищенных ЦСПИ необходимо использовать концепцию «цифрового радио» *SDR* (*Software Digital Radio*), представляющую собой программно-аппаратную платформу, в которой интегрированы сетевой процессор *NP*, блок потоковой цифровой обработки сигналов на основе программируемой логической матрицы *FPGA*, аналого-цифровые АЦП и цифро-аналоговые преобразователи ЦАП.

На рис. 3. показана структура *SDR* для обработки многомерных сигналов в *MIMO* канале связи с *N* передатчиками *T* и *N* приемниками *R*.

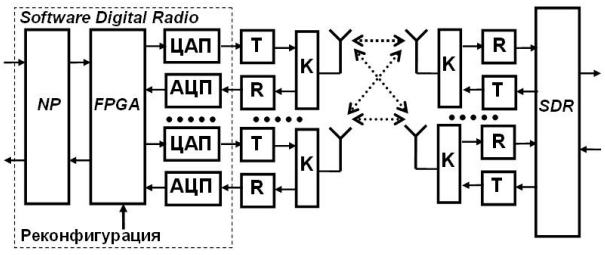

Рис. 3 — Структурная схема программно-аппаратной платформы *SDR*

Учитывая большое различие в принципах работы беспроводных технологий передачи информации, изменение только программного обеспечения (ПО) *SDR* недостаточно для эффективной интеграции, поэтому необходима еще достаточно сложная реконфигурация аппаратных средств, реализующих взаимодействие абонентов сети на канальном уровне.

Для оценки возможностей существующих программно-аппаратных платформ нами был разработан цифровой блок обработки широкополосных сигналов с большой базой с использованием платформы разработчика *DK-DSP-2C70N* (*Altera*) [9].

Как известно, одним из эффективных методов обработки широкополосного сигнала на приеме является согласованная фильтрация, которая максимизирует отношение сигнал-шум в канале связи. Программируемый цифровой согласованный фильтр для свертки сигналов в частотной области является одним из наиболее сложных для реализации элементов помехозащищенной ЦСПИ. Это обусловлено необходимостью очень высокого быстродействия спецпроцессора, которая для сигнала с базой более *1000* становится проблематичной даже при использовании самых современных сигнальных процессоров и *FPGA*.

Общая структурная схема устройства цифровой обработки сложных широкополосных сигналов на основе *FPGA* показана на рис. 4. Данная схема реализует принцип свертки сложного сигнала в частотной области, включая режекцию узкополосных помех, и формирует квадрат модуля свертки отсчетов принимаемого сигнала и двух опорных последовательностей *PN1* и *PN2*.

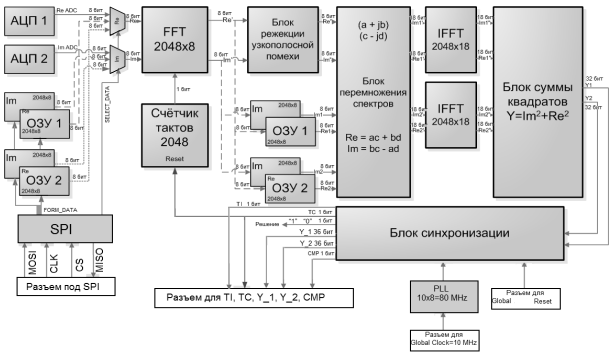

Рис. 4 — Обобщенная структурная схема блока цифровой обработки широкополосных сигналов

На осциллограмме (рис. 5) показано положение автокорреляционной функции *АКФ* входного сигнала по отношению к тактовому импульсу *ТИ*, поступающего с выхода блока синхронизации, при отношении сигнал-шум SNR_{INP}= *–6 дБ* на входе фильтра.

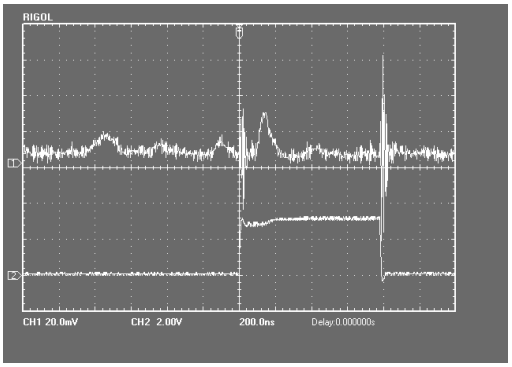

Рис. 5 — Осциллограмма АКФ на выходе устройства при отношении сигнал-шум *SNR= –6 дБ*

Как видно из осциллограммы отношение сигнал/шум на выходе фильтра составляет около SNR_{OUT} = *12 дБ*, а общая эффективность цифровой обработки широкополосного сигнала составляет *18 дБ* (защищенность системы).

Для повышения энергетического потенциала легитимного канала связи важно также знать параметры затухания РРВ в канале связи при различном

пространственном расположении абонентов в зоне доступа. Эффективная работа адаптационного алгоритма настройки ЦСПИ напрямую зависит от оценки параметров канала связи в реальном масштабе времени, что требует разработки упрощенных моделей для реализации их на программно-аппаратной платформе *SDR*.

В ХНУРЭ разработано целый ряд программ моделирования беспроводных каналов связи уровня *LAN* и *MAN*. Они основаны на отражательной трактовке и использовании метода микроволновых волновых каналов, что дает возможность с достаточно высокой точностью прогнозировать параметры и производительность канала связи в зоне развертывания системы радиодоступа [10, 11].

В докладе рассматривается пример создания отечественного защищенного центра обслуживания вызовов (ЦОВ) службы «102» ГУМВД [12].

Основной отличительной особенностью разработанной ВСС является использование сетевой инфраструктуры на основе существующих отечественных КЛС и расширение пропускной способности проводных каналов связи за счет разработки и внедрения новых защищенных многоканальных ЦСПИ *«Quadro»* на основе симметричных *SHDSL* технологий, в которых реализована интеграция процессов кодирования, модуляции, шифрования, преобразования и обработки сигналов в одном едином цифровом процессе обработки [13].

На рис. 5 показана распределенная архитектура ЦОВ службы «102» ГУВМД г. Харькова.

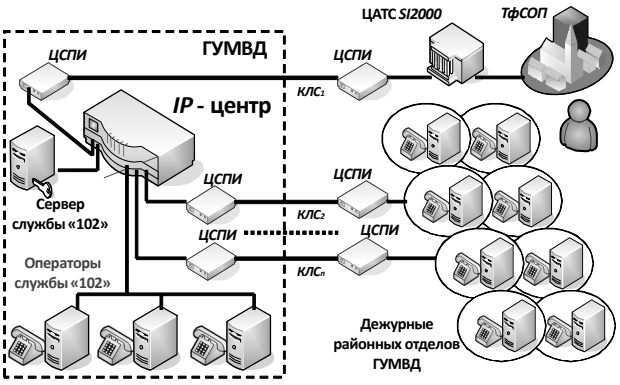

Рис. 5 — Обобщенная структурная схема ЦОВ службы «102» ГУМВД г. Харькова

Структура ЦОВ включает в себя нескольких подсистем и сетей: станционное оборудование (ЦАТС) службы «102», центральный информационный сервер (ЦИС) службы «102», рабочие места оператора (РМО) службы «102», сеть проводного доступа (СПД) для связи станционного оборудования службы «102» с районными отделениями ГУМВД на основе ЦСПИ и с узлом экстренных и информационно-справочных служб Харьковского филиала ОАО «Укртелеком», рабочие места дежурных (РМД) районных отделений ГУМВД.

Оперативность принятия вызовов, своевременное информирование о происшествиях дежурных в районных отделениях ГУМВД дало возможность более оперативно и качественно реагировать и раскрывать преступления по «горячим» следам.

3. Заключение

1) Из изложенного в докладе материала следует, что характерной особенностью современного уровня научно-технического прогресса в области развития ЦСПИ является интеграция технологий, в том числе и в сфере защиты информации, и эта тенденция в дальнейшей перспективе будет сохраняться и углубляться.

2) Энергетический уровень различных технологий передачи информации несет большой потенциал, который может быть использован для повышения безопасности в сетях доступа.

3) Перспективным направлением повышения энергетической защищенности каналов связи ЦСПИ является использование *MIMO*-технологий и многомерного пространства сигналов.

4. Список литературы

[1] Шокало В.М. Концепция создания отечественных специальных цифровых систем передачи информации / В.М. Шокало, А.И. Цопа // Наук.-техн. журнал «Захист інформації». — Київ: ДУІКТ, 2006. — № 3. — С. 51 — 57.

[2] Коваль Ю.А. Развитие теории и совершенствование метеорных систем связи и синхронизации / Ю.А. Коваль, В.В. Бавыкина. — Харьков: Коллегиум, 2006. — 308 с.

[3] Защищенные радиосистемы цифровой передачи информации / П.Н. Сердюков, А.В. Бельчиков, А.Е. Дронов и др. — М.: АСТ, 2006. — 403 с.

[4] Shannon K. Communication theory of secrecy systems / K. Shannon // Bell Systems Tech Journal. — 1949. — Vol. 28, № 4. — P. 656 — 715.

[5] Котельников В.А. Теория потенциальной помехоустойчивости / В.А. Котельников. — М.: ГЭИ, 1956. — 151 с.

[6] Зюко А.Г. Помехоустойчивость и эффективность систем связи / А.Г. Зюко. — М.: Связь, 1972. — 360 с.

[7] Wyner A.D. The wire-tap channel / A.D. Wyner // Bell System Technical Journal. — 1975. — Vol. 54, № 8. — P. 1355 — 1387.

[8] Ozarow L.Y. Wire-Tap channel II / L.Y. Ozarow, A.D. Wyner // AT&T Bell labs Technical Journal. — 1984. — Vol. 3. — P. 2135 — 2157.

[9] Signal Processing Verification System Programmable Digital Matched Filter / O.I.Tsopa [et al.] // Proc. 6-th IEEE East-West Design & Test Symposium «EWDTS-2008». — Lviv (Ukraine), 2008. — P. 243 — 250.

[10] Вариант модели затухания широкополосного сигнала в радиолинии при расчете защищенности локальной сети связи / А.А. Стрельницкий, А.Е. Стрельницкий, А.И. Цопа, В.М. Шокало // Науч.-техн. журнал «Захист інформації». — Киев: ГУИКТ, 2008. — №3(39). — С. 38 — 43.

[11] Shokalo V.M. Approximate Model for Estimation of Efficiency and Noise Immunity of Branched Street and Corridor Wi-Fi and WiMAX Communication Channels / A.A. Strelnitskiy, O.I. Tsopa // International journal «Telecommunication and Radio Engineering». — Begell House, 2009. — Vol. 68(17). — P. 1511 — 1528.

[12] Цопа А.И. Направления создания защищенных центров обслуживания вызовов службы «02» УМВД Украины / В.В. Маслий, А.И. Цопа // Наук.-техн. журнал «Захист інформації». — Київ: ДУІКТ, 2007. — № 4. — С. 87 — 92.

[13] Цопа А.И. Оценка предельной производительности проводных каналов связи с различными *xDSL* технологиями / А.И. Цопа // Радиотехника. Всеукраинский межведомственный науч.-техн. сборник. — 2009. — № 159. — С. 36 — 45.